Beyond Ethereal: Crafting A Tivo for Security Datastreams

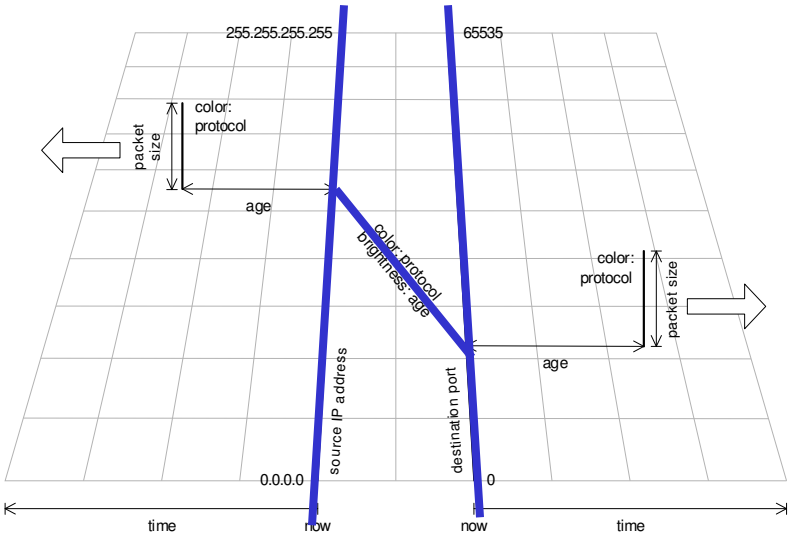
Gregory Conti
www.cc.gatech.edu/~conti
conti@cc.gatech.edu

Disclaimer

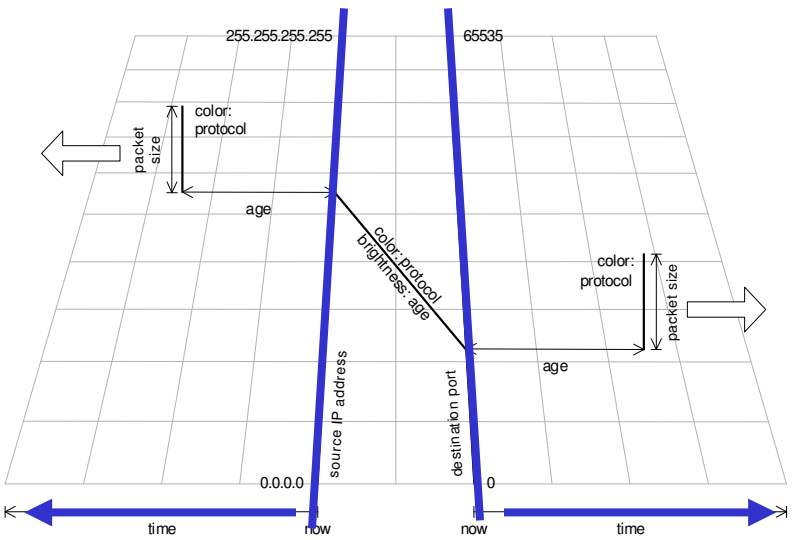
The views expressed in this presentation are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.

image: http://www.leavenworth.army.mil/usdb/standard%20products/vtdefault.htm

One Possible View



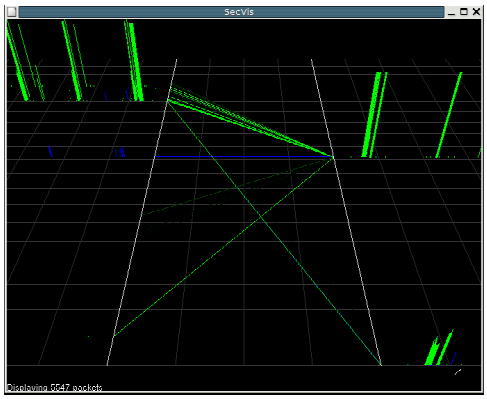
One Possible View



SecVis Demo

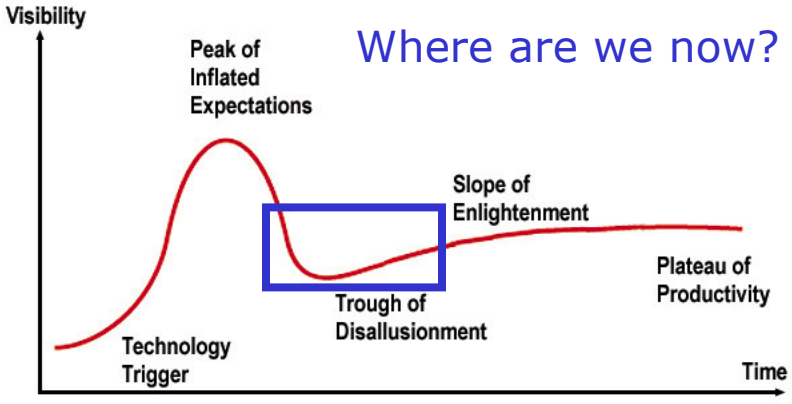
(one possible window)

- Sven Krasser design and implementation lead
- Code on CD
  - Caveats
  - Thanks to NETI@Home
  - Released under GPL
- See the research paper for more information



demo

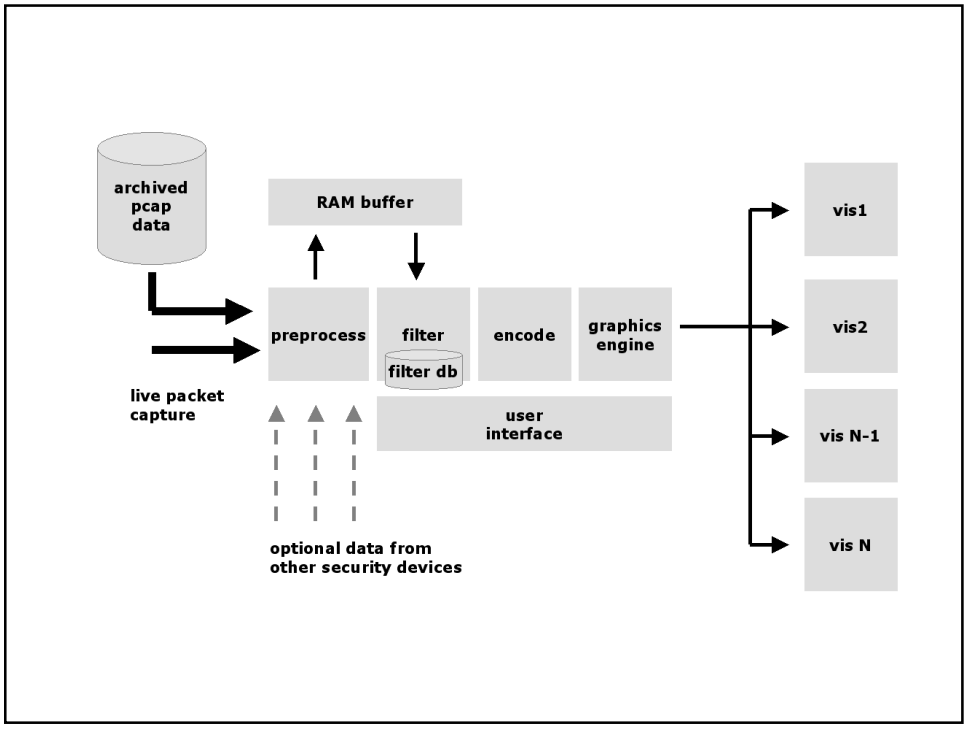
Gartner's Hype Cycle

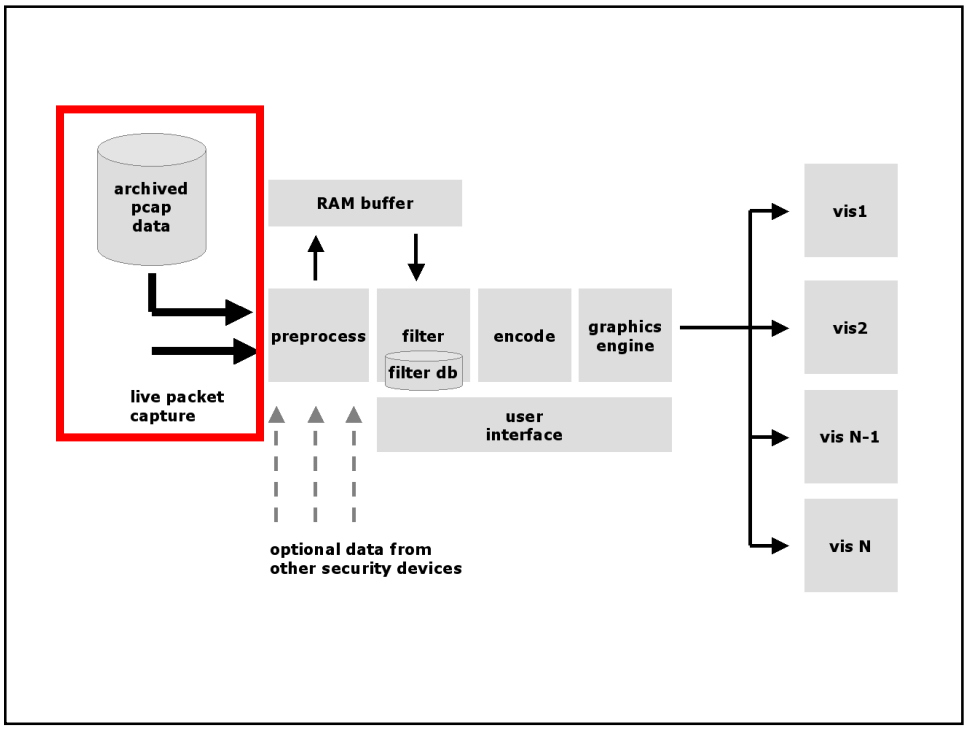


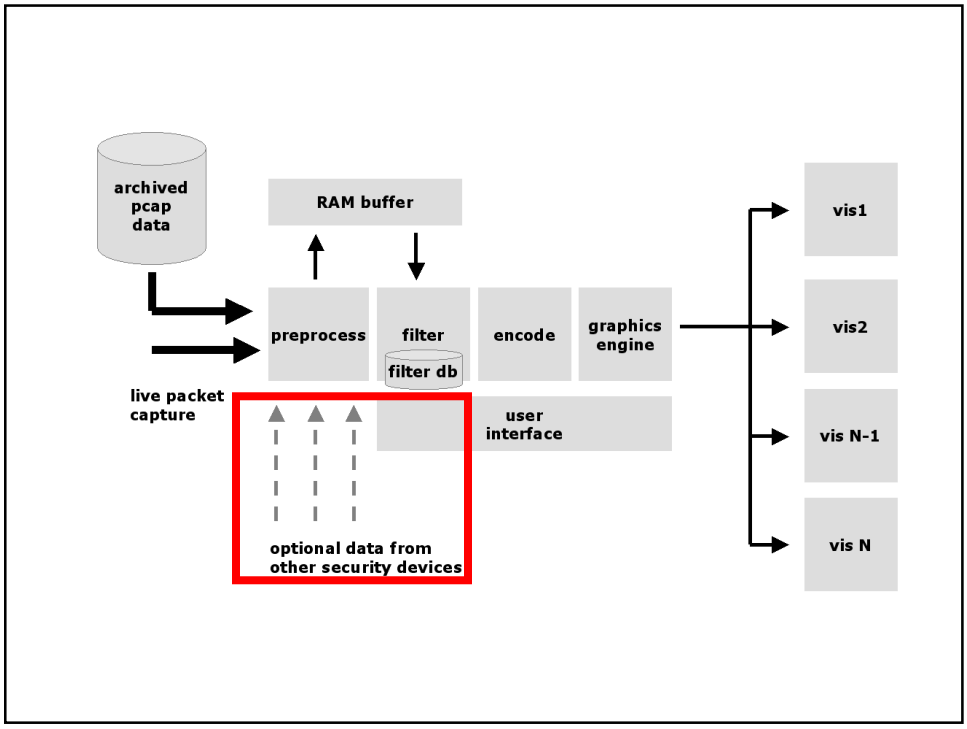
Where are we now?

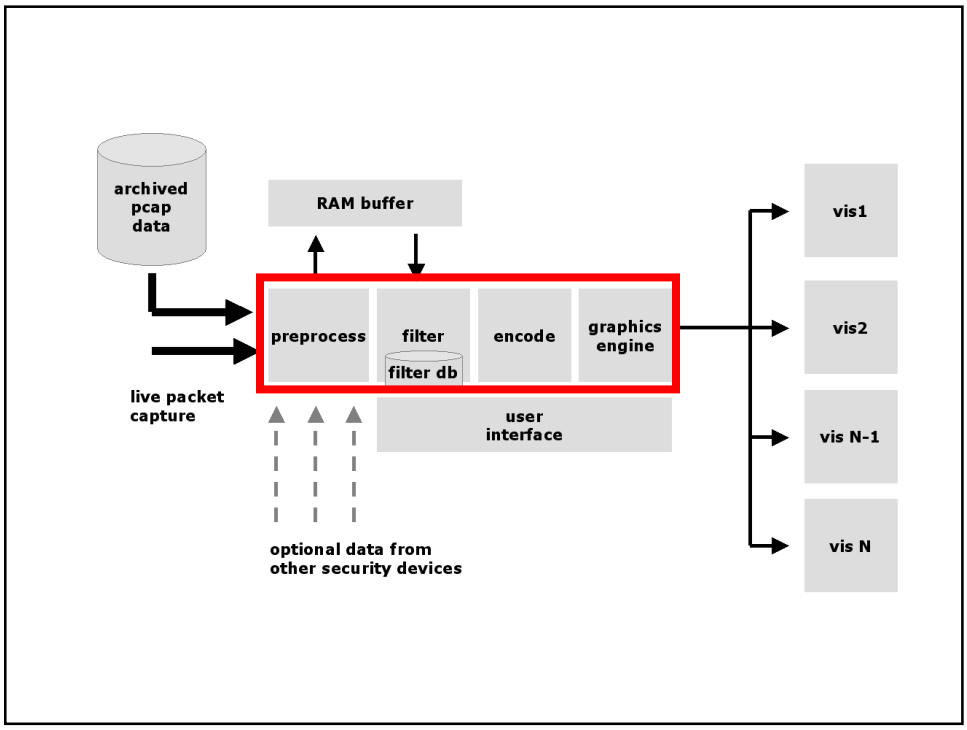
-Gartner Group

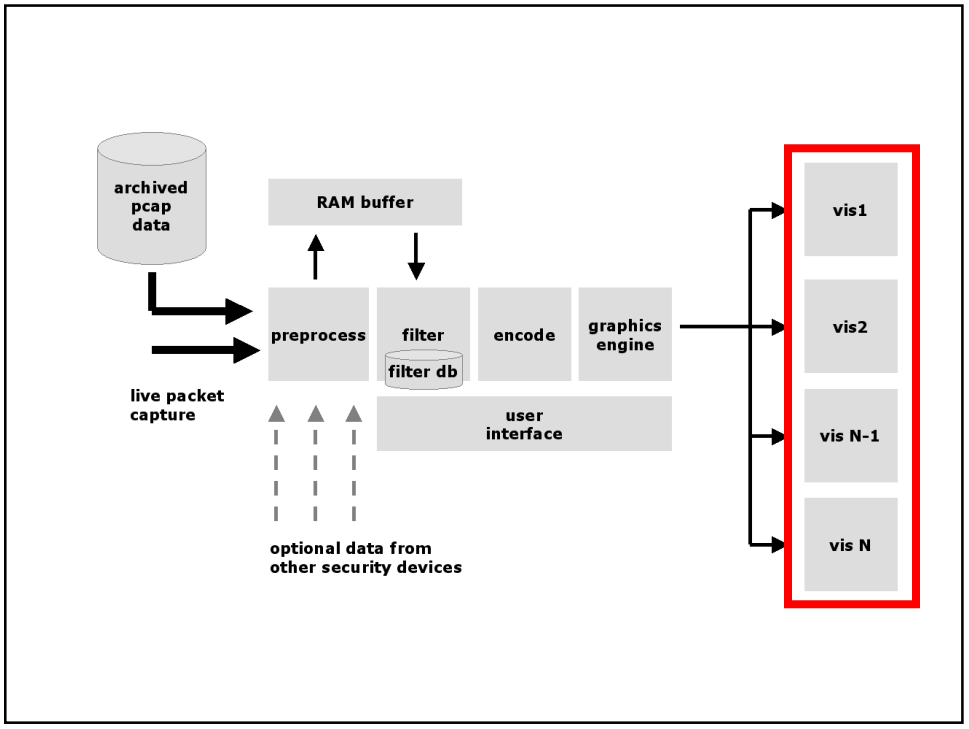
Thanks go to Kirsten Whitely for the Gartner curve idea
http://java.sun.com/features/1998/03/images/year3/original/gartner.curve.jpg

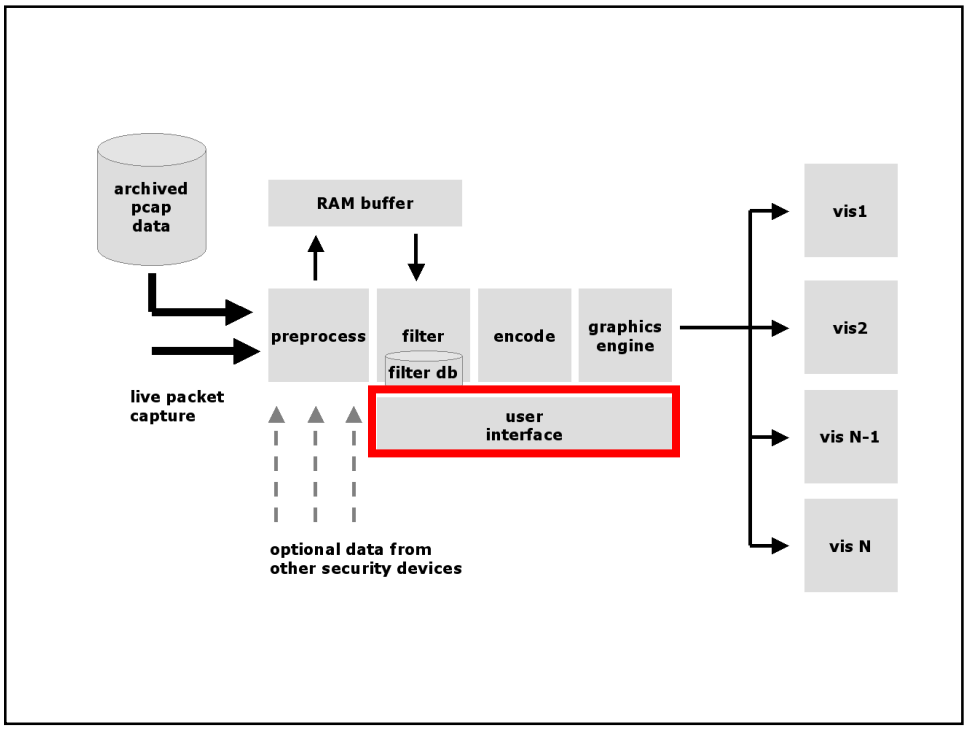

archived pcap data
RAM buffer
preprocess
filter
filter db
encode
graphics engine
vis1
vis2
vis N-1
vis N
live packet capture
user interface
optional data from other security devices


archived pcap data
RAM buffer
preprocess
filter
filter db
encode
graphics engine
vis1
vis2
vis N-1
vis N
live packet capture
user interface
optional data from other security devices


archived pcap data
RAM buffer
preprocess
filter
filter db
encode
graphics engine
vis1
vis2
vis N-1
vis N
live packet capture
user interface
optional data from other security devices


archived pcap data
RAM buffer
preprocess
filter
filter db
encode
graphics engine
vis1
vis2
vis N-1
vis N
live packet capture
user interface
optional data from other security devices


archived pcap data
RAM buffer
preprocess
filter
filter db
encode
graphics engine
vis1
vis2
vis N-1
vis N
live packet capture
user interface
optional data from other security devices


archived pcap data
RAM buffer
preprocess
filter
filter db
encode
graphics engine
vis1
vis2
vis N-1
vis N
live packet capture
user interface
optional data from other security devices

Potential DataStreams

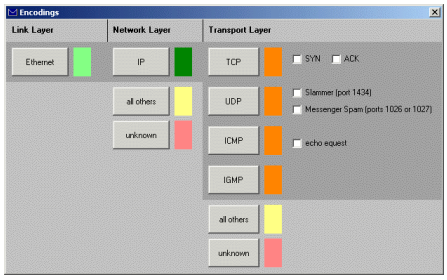
- Traditional
  - pcap
  - snort
  - syslog
  - firewall logs
  - anti-virus
  - reconstruct streams
  - …
- Less traditional
  - p0f
  - IANA data (illegal IP's)
  - reverse DNS
  - local data (unassigned local IPs)
  - inverted snort
  - active tools (e.g. nmap)
  - …

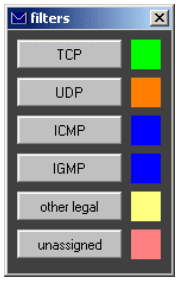
- **packet length (from Winpcap)**
- **Ethertype**
- **IP Transport Protocol**
- **Source/Destination IP**
- **TTL**
- **IP Header Len**
- **IP Version**
- **IP Diff Services**
- **IP Total Length**
- **IP Identification**
- **IP Flags**
- **IP Fragment Offset**
- **IP Header Checksum**
- **UDP Source/Destination Port**
- **TCP Source/Destination Port**

RUMINT Main Screen

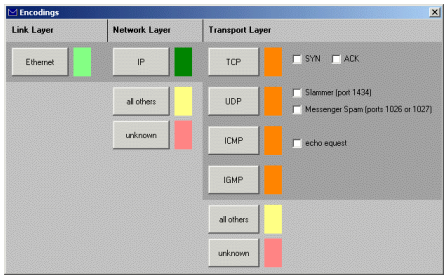
- Provide quick overview with minimal clutter
- Thumbnails act as menu
- Why "RUMINT"

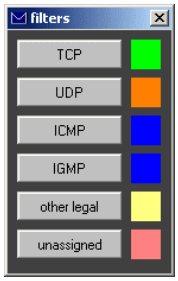
Filtering, Encoding & Interaction

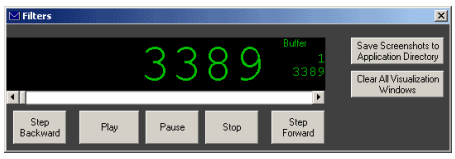




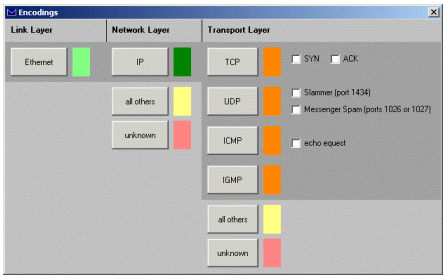
Filtering, Encoding & Interaction

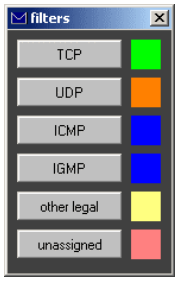


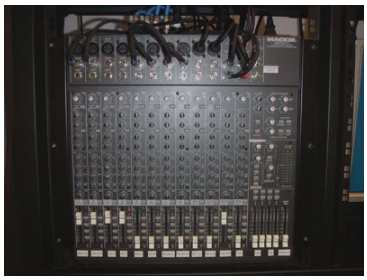




Filtering, Encoding & Interaction







For More Information…

- **Dynamic Queries**
  - Ben Shneiderman. http://www.cs.umd.edu/hcil/spotfire/
- **Requirements and Tasks**
  - Goodall. User Requirements and Design of a Visualization for Intrusion Detection Analysis
  - Komlodi, Goodall and LuttersAn Information Visualization Framework for Intrusion Detection. http://userpages.umbc.edu/~jgood/publications/komlodi-chi04.pdf
- **Semantic Zoom**
  - Bederson, et al., "Pad++: A Zoomable Graphical Sketchpad for Exploring Alternate Interface Physics," Journal of Visual Languages and Computing, 1996, Volume 7, pages 3-31. http://citeseer.ist.psu.edu/bederson95pad.html
- **Noise in Internet Data**
  - Pang, Yegneswaran, Barford, Paxson and Peterson. Characteristics of Internet Background Radiation. www.icir.org/vern/papers/radiation-imc04.pdf
  - Grizzard, Simpson, Krasser, Owen and Riley. Flow Based Observations from NETI@home and Honeynet Data. www.ece.gatech.edu/research/labs/nsa/papers/neti-honey.pdf
- **Automatic Filter Generation**
  - Lakkaraju, Bearavolu, Slagell and Yurcik. Closing-the-Loop: Discovery and Search in Security Visualizations. http://www.ncassr.org/projects/sift/papers/westpoint05_closing-the-loop.pdf
- **Human in the Loop Systems**
  - Korzyk and Yurcik. On Integrating Human In the Loop Supervision into Critical Infrastructure Process Control Systems. www.ncassr.org/projects/sift/papers/astc2002_humaninloop.pdf
  - Su and Yurcik. "A Survey and Comparison of Human Monitoring of Complex Networks." http://www.ncassr.org/projects/sift/papers/iccrts05.pdf

Binary Rainfall Visualization

(single packet)

Bits on wire…

0	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1	1	1	0

Binary Rainfall Visualization

(single packet)

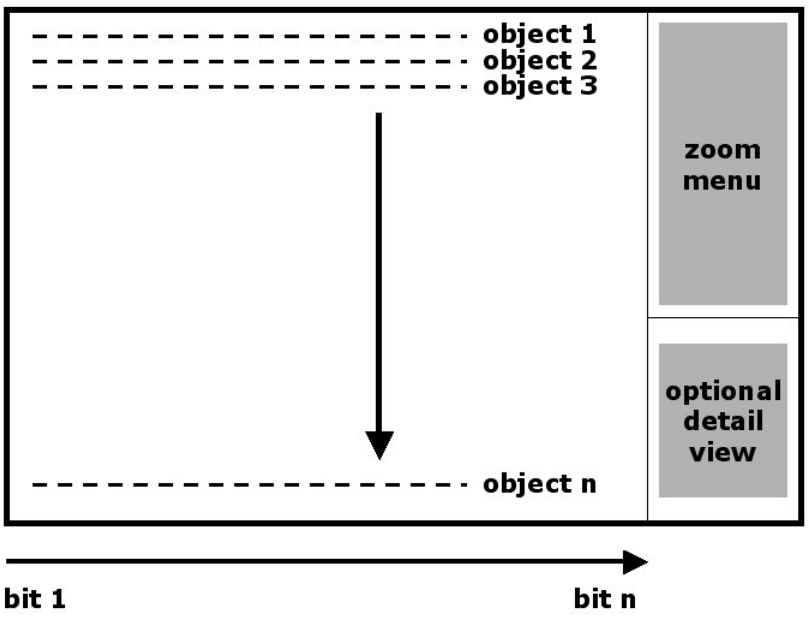
Bits on wire…

0	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1	1	1	0

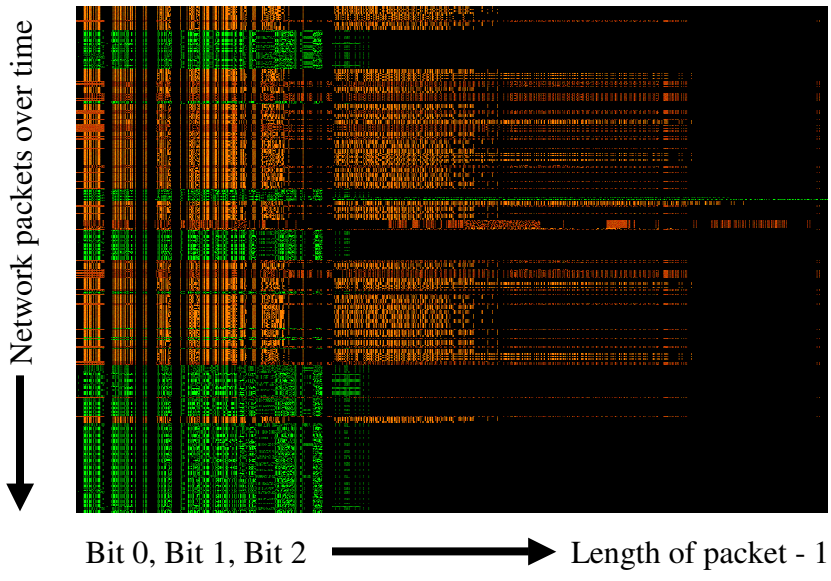
View as a 1:1 relationship (1 bit per pixel)…

0	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1	1	1	0

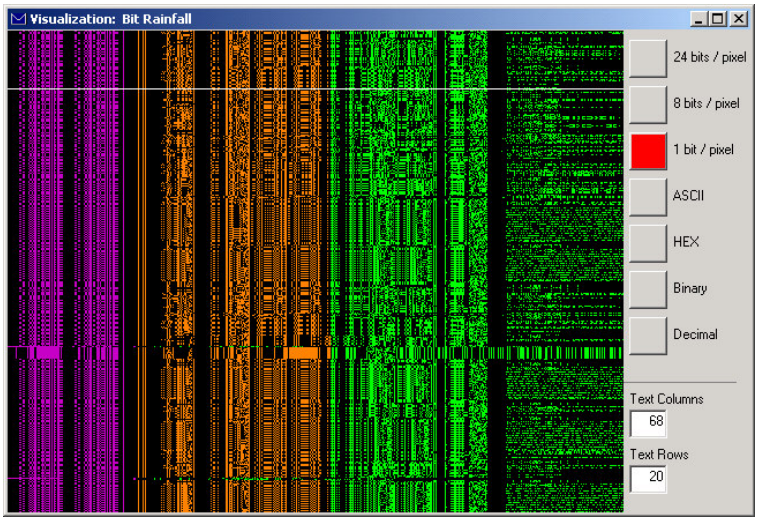
24 Pixels



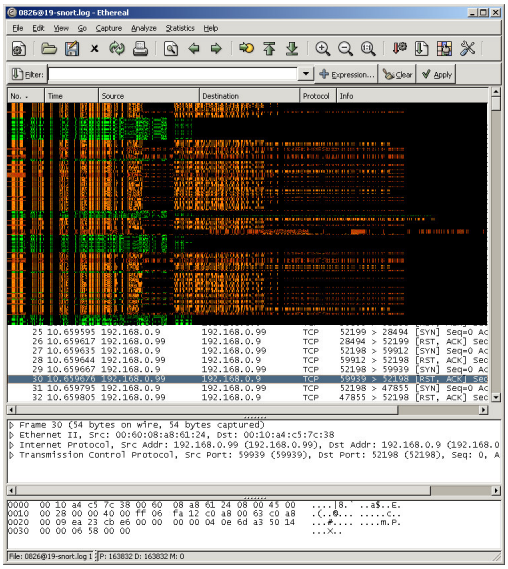
Encode by Protocol



Encoding Headers



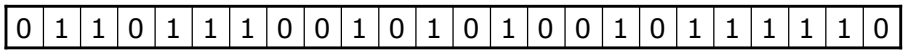
Navigation



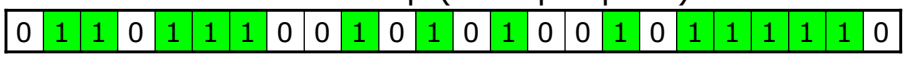
Binary Rainfall Visualization

(single packet)

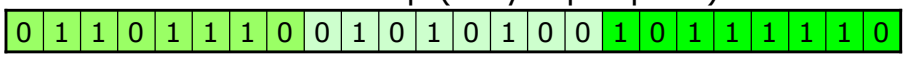
Bits on wire…



View as a 1:1 relationship (1 bit per pixel)…



View as a 8:1 relationship (1 byte per pixel)…

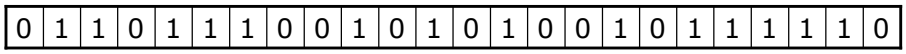


3 Pixels

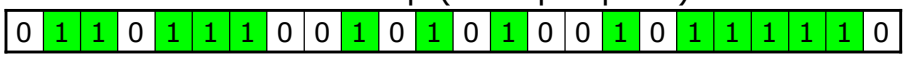
Binary Rainfall Visualization

(single packet)

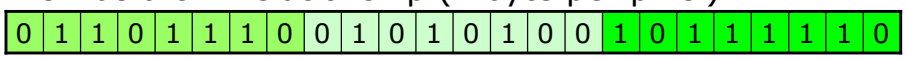
Bits on wire…



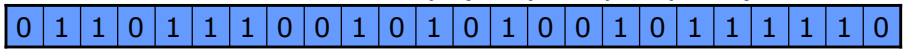
View as a 1:1 relationship (1 bit per pixel)…



View as a 8:1 relationship (1 byte per pixel)…

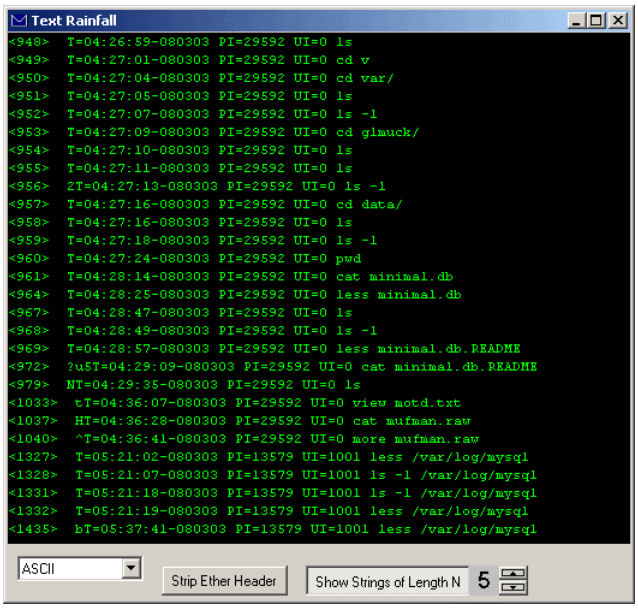


View as a 24:1 relationship (3 bytes per pixel)…



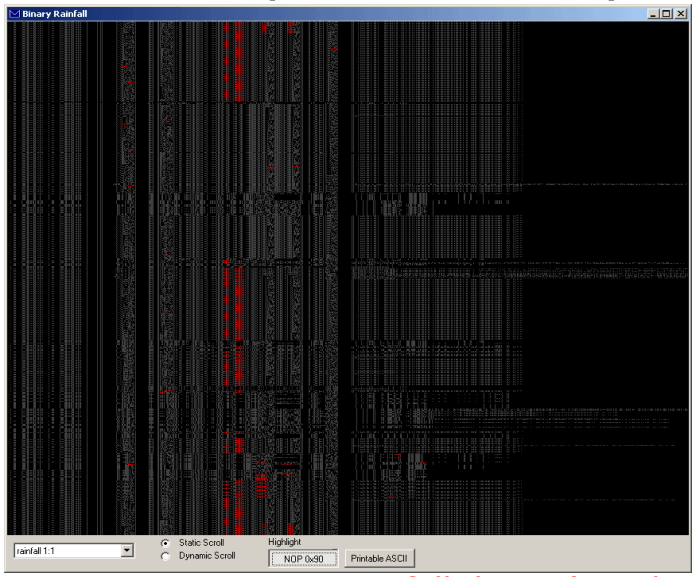
1 Pixel

On the fly *strings*



dataset: Defcon 11 CTF

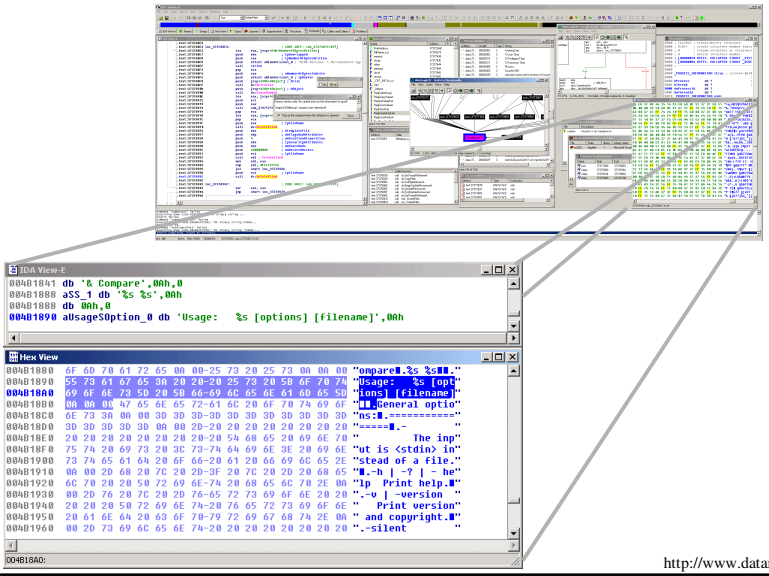
On the fly *disassembly*?



rainfall demo (graphic & text)

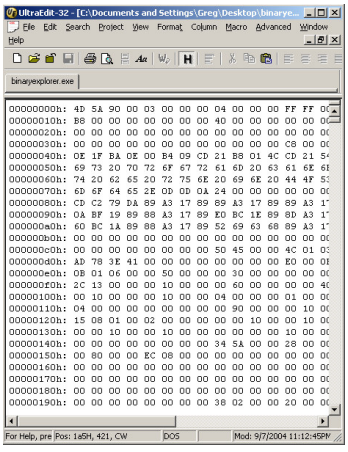
dataset: Honeynet Project Scan of the Month 21

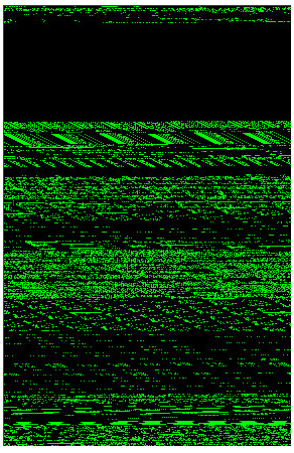
A Variant:
Visual Exploration of Binary Objects



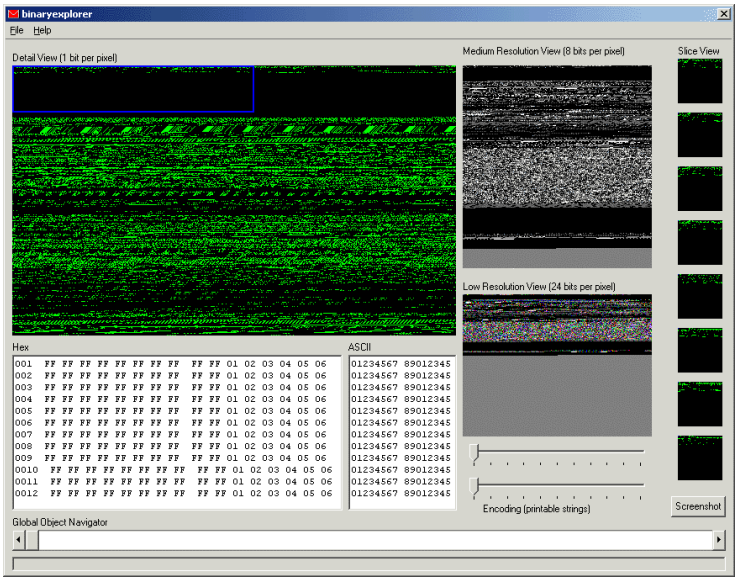
http://www.datarescue.com/idabase/

Textual vs. Visual Exploration



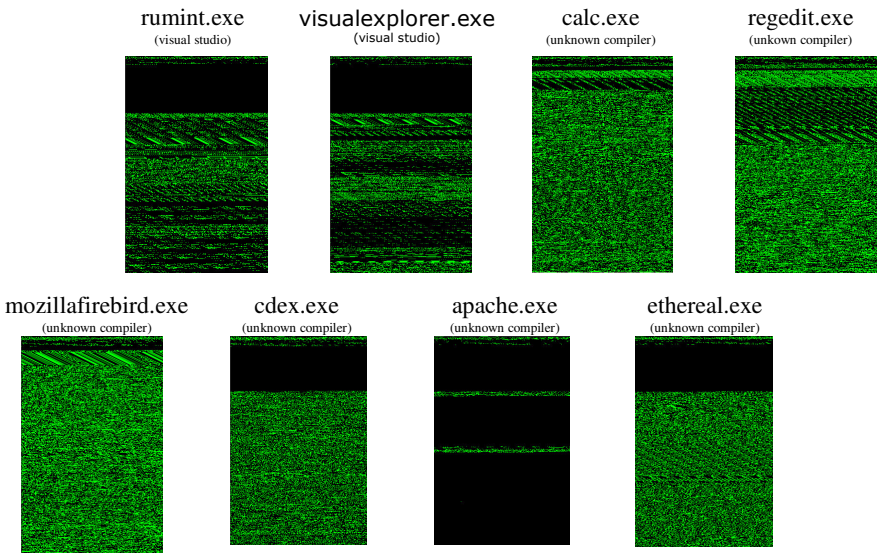


binaryexplorer.exe



Comparing Executable Binaries

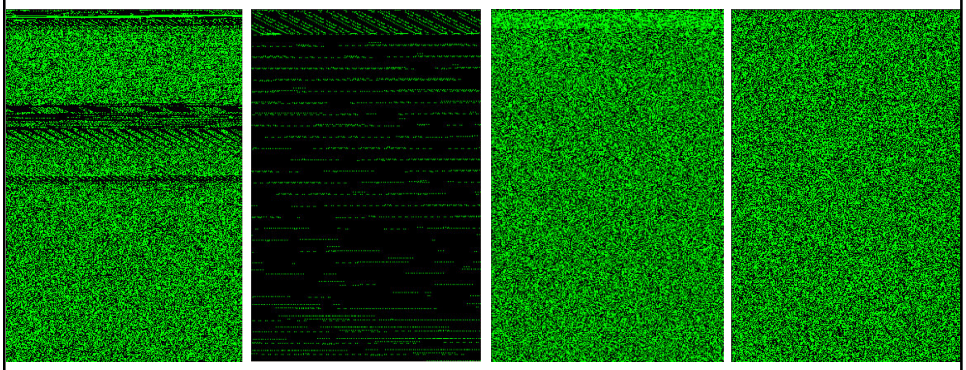
(1 bit per pixel)



Comparing Image Files

(1 bit per pixel)

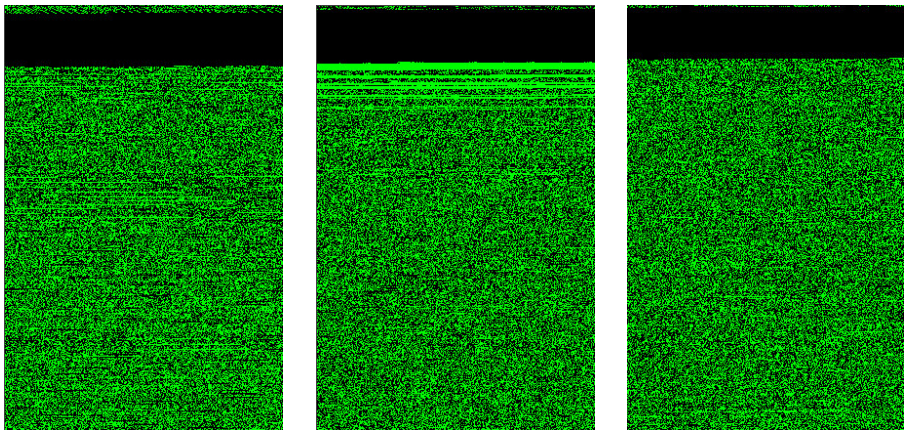
image.jpg | image.bmp | image.zip | image.pae (encrypted)



Comparing mp3 files

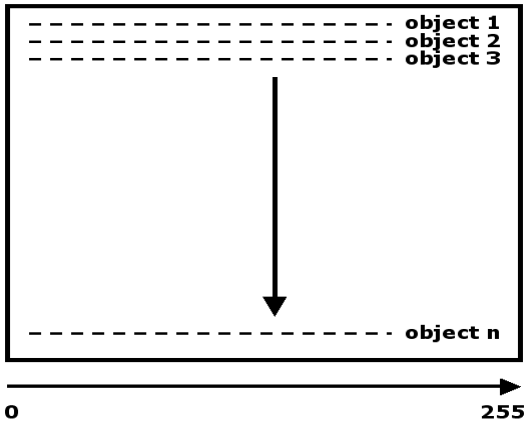
(1 bit per pixel)

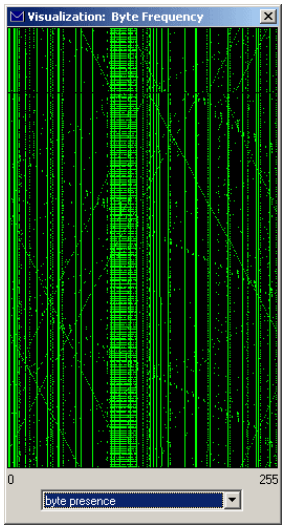
the.mp3 | pash.mp3 | disguises.mp3



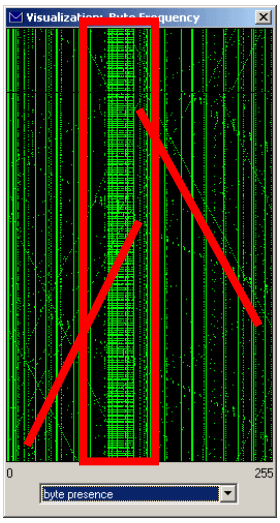
binary explorer demo

Byte Visualization

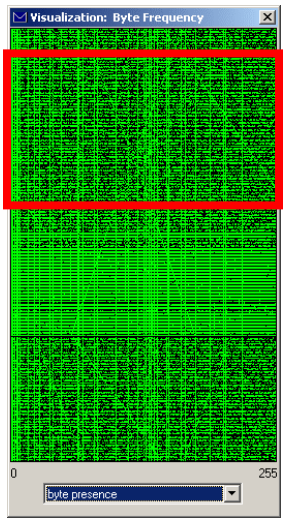




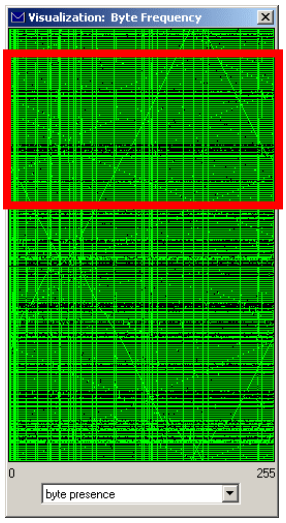
Byte Presence



dictionary file via HTTP

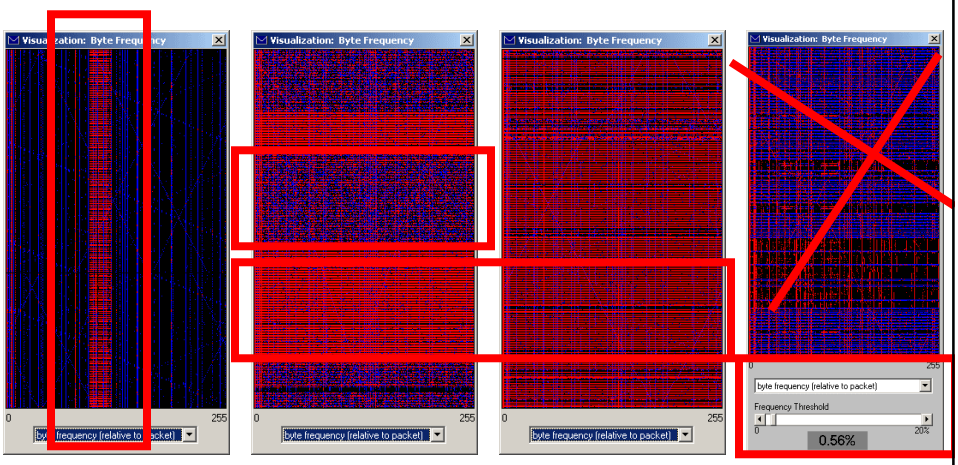


ssh



SSL

Byte Frequency



dictionary file over HTTP

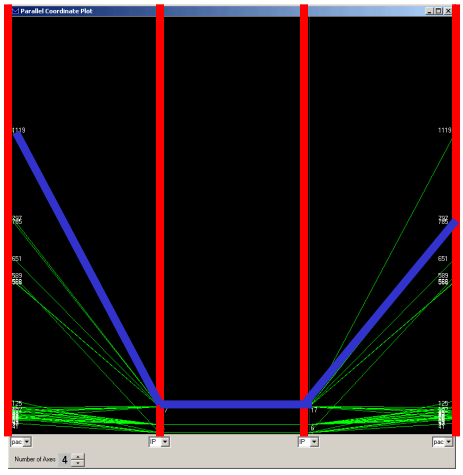
ssh

SSL

streaming audio

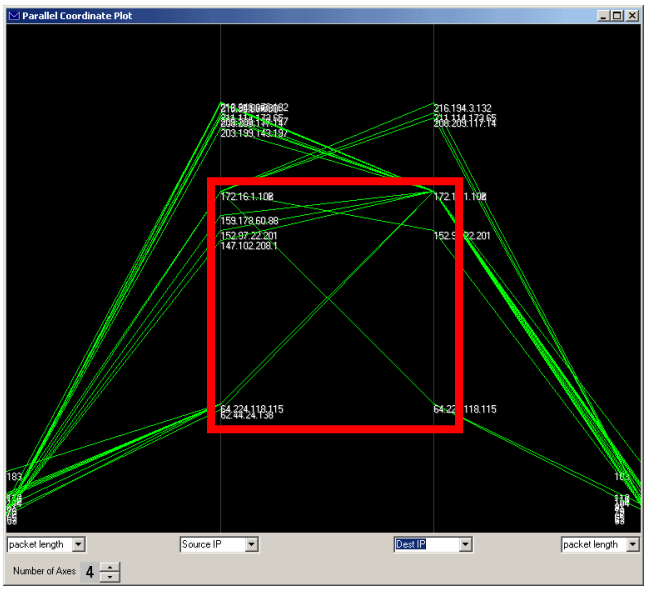
byte frequency demo

Parallel Coordinates



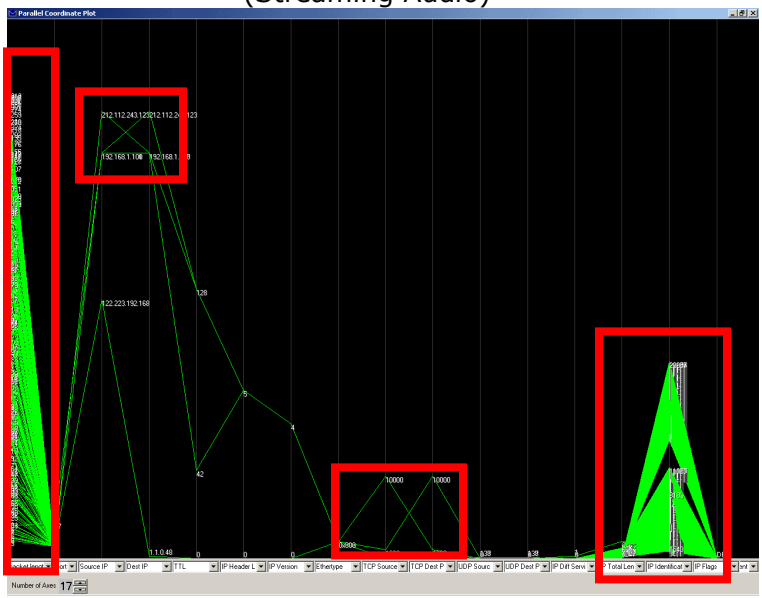
- goal: plot any data fields
- dynamic columns
- change order for different insight
- intelligent lookup and translation of fields
  - e.g. IP transport protocol

Parallel Coordinates



Parallel Coordinates

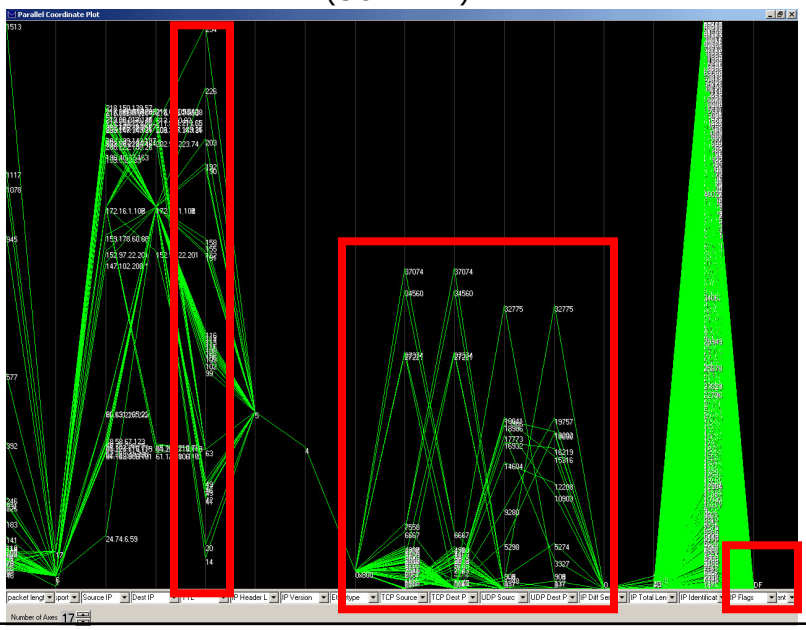
(Streaming Audio)



Parallel Coordinates

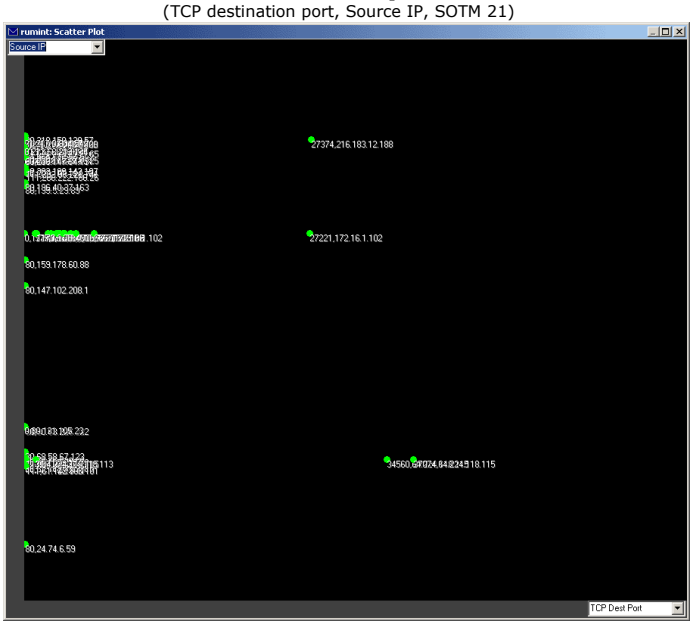
demo

(SOTM 21)

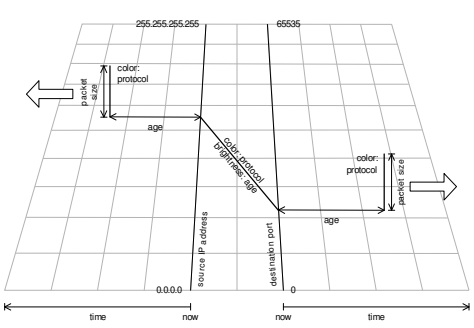


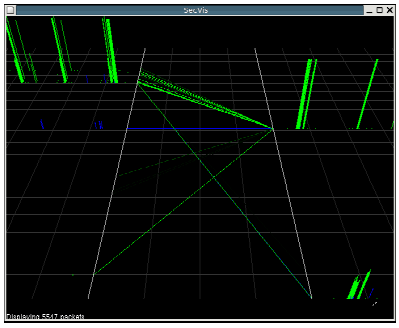
Scatterplot

(TCP destination port, Source IP, SOTM 21)

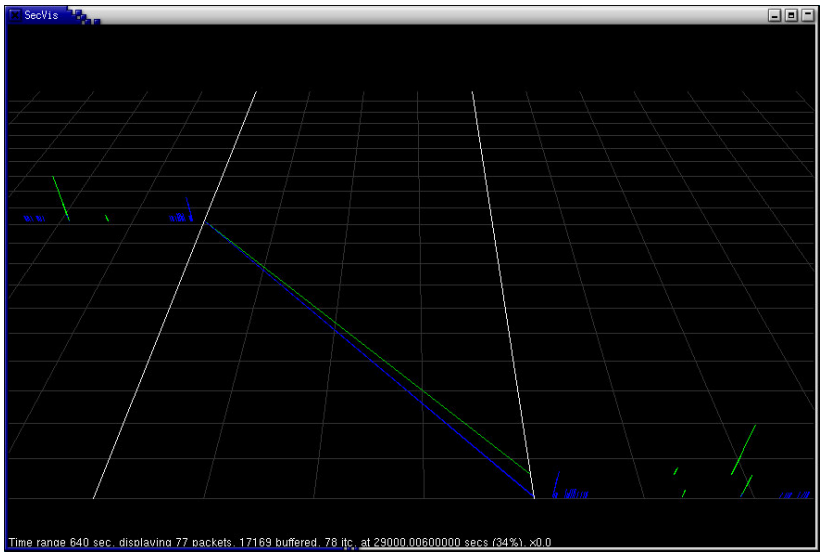


Krasser Visualization
(secvis)

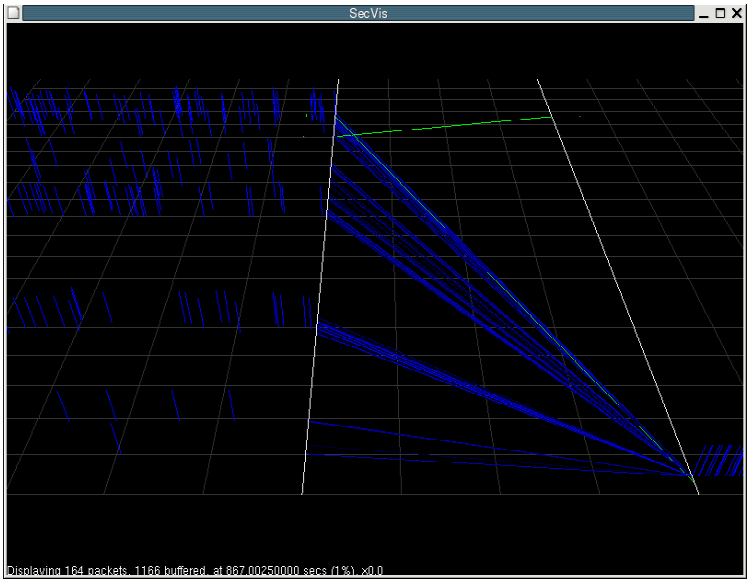




Routine Honeynet Traffic
(baseline)

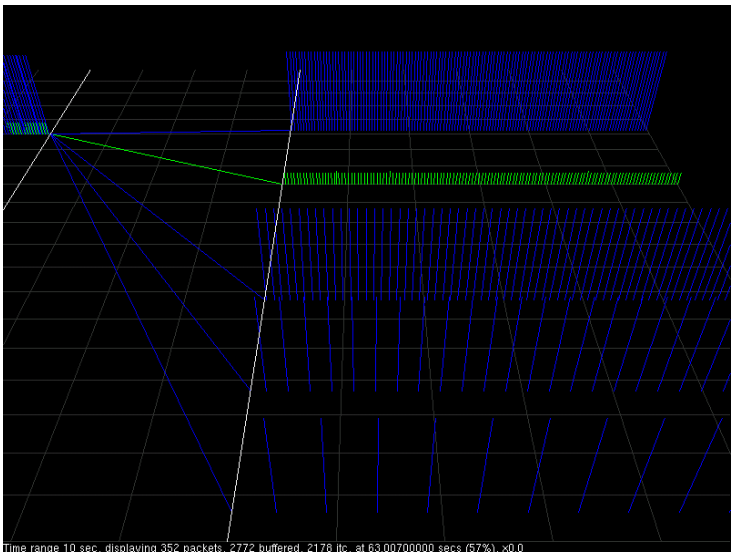


Slammer Worm

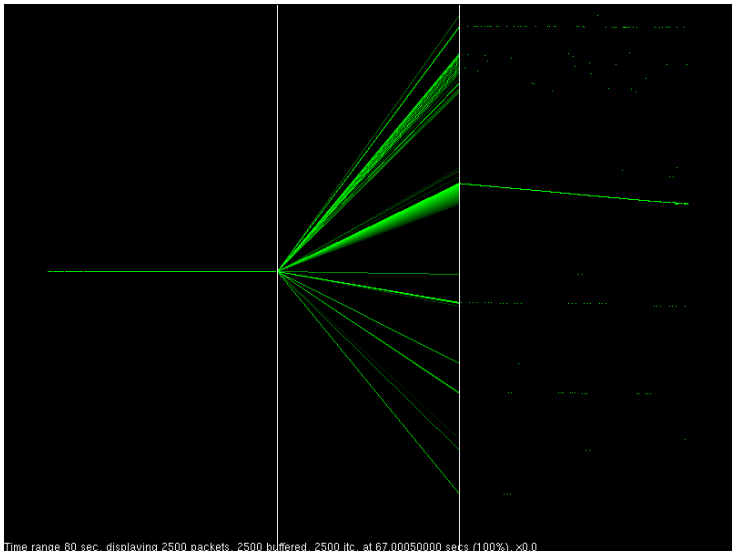


At a Glance Measurement

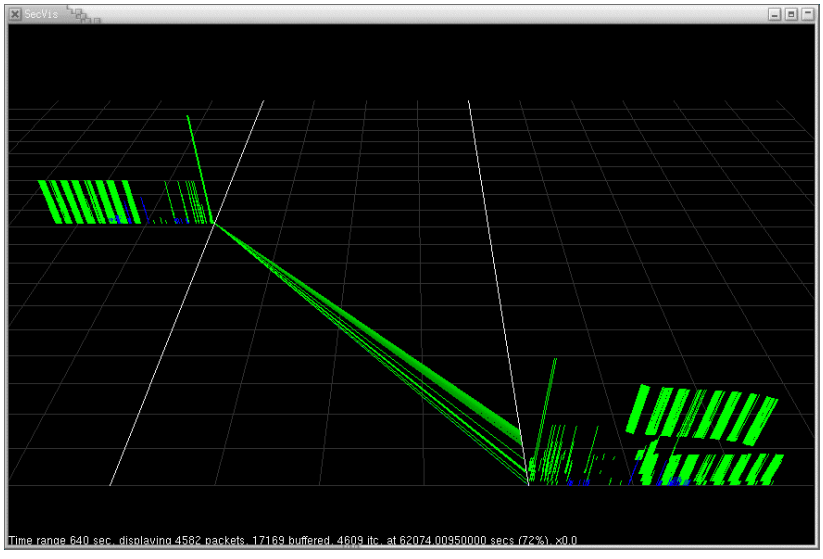
(Constant Bitrate UDP Traffic)



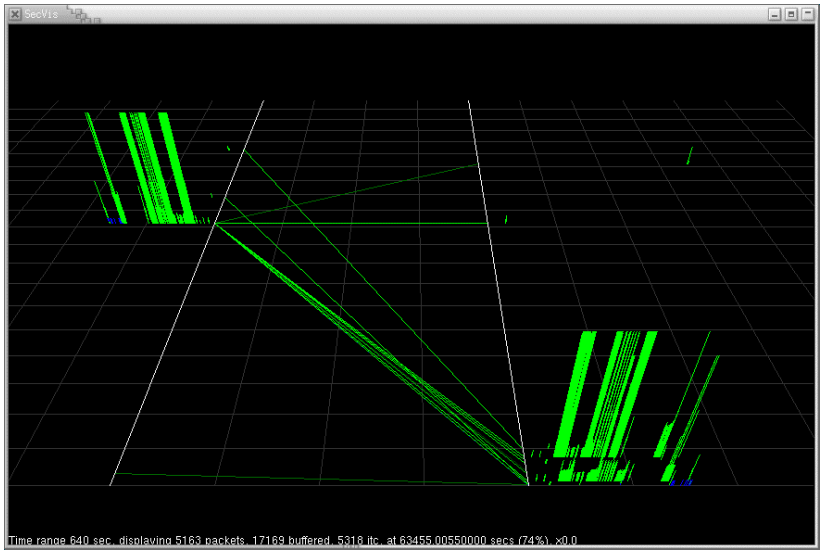
Port Sweep



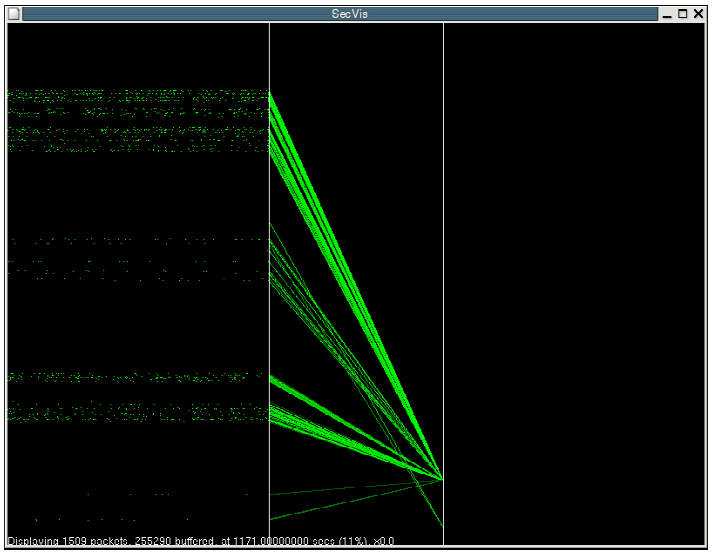
Compromised Honeypot



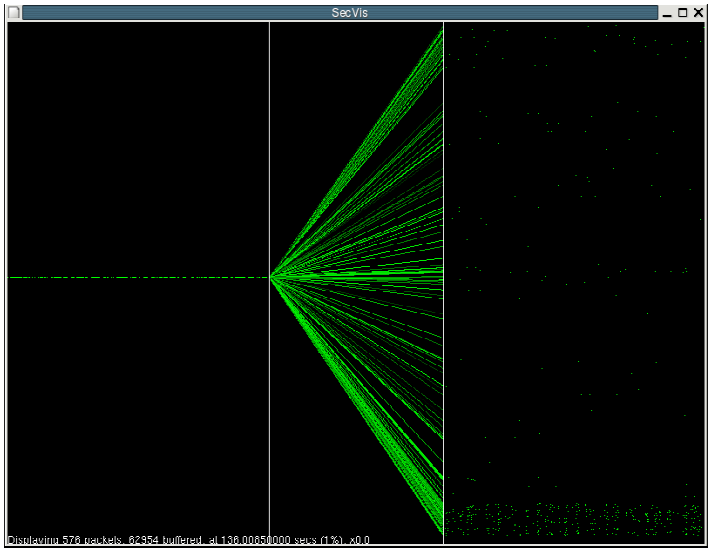
Attacker Transfers Three Files…



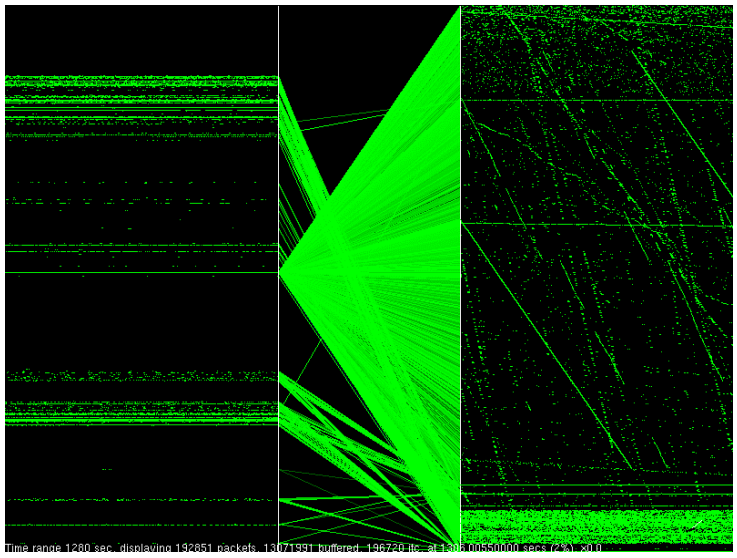
Inbound botnet Traffic



Outbound botnet Traffic



Combined botnet/honeynet traffic



For more information…

Bit Rainfall (email me…)

- G. Conti, J. Grizzard, M. Ahamad and H. Owen; "Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries;" IEEE Symposium on Information Visualization's Workshop on Visualization for Computer Security (VizSEC); October 2005.

Parallel Coordinate Plots

- Multidimensional Detective by Alfred Inselberg http://www.sims.berkeley.edu/academics/courses/is247/s04/resources/inselberg97.pdf

Byte Frequency Analysis

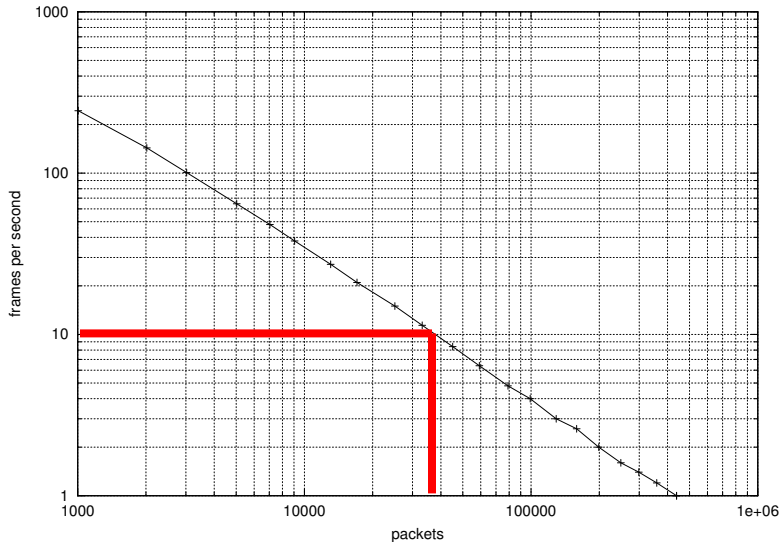
- Wei-Jen Li, Benjamin Herzog, Ke Wang, Sal Stolfo , " Fileprints: Identifying File Types by N-gram Analysis", IEEE Information Assurance Workshop, 2005.
- Ke Wang, Salvatore J. Stolfo. "Anomalous Payload-based Network Intrusion Detection", *Recent Advance in Intrusion Detection (RAID), 2004*.

Krasser Visualization (see www.cc.gatech.edu/~conti)

- S. Krasser, G. Conti, J. Grizzard, J. Gribschaw and H. Owen; "Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization;" *IEEE Information Assurance Workshop (IAW)*; June 2005.

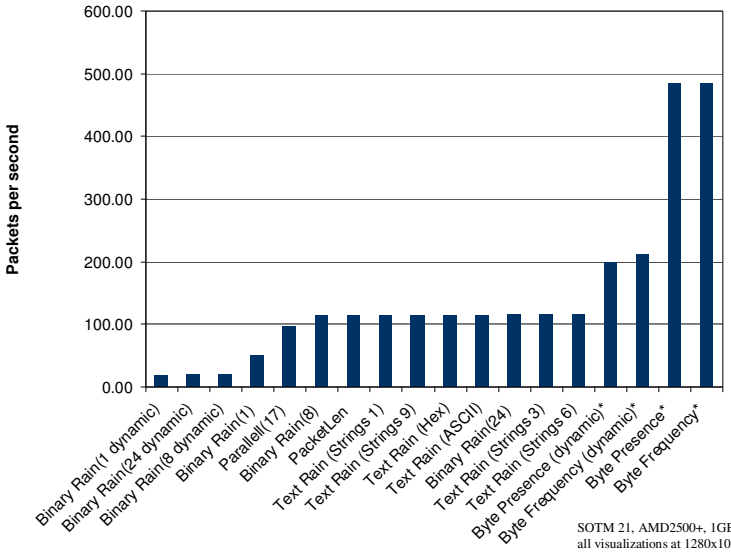
Raffael Marty @ DEFCON

Open GL System Performance
(secvis)



Win32 Performance

(SOTM 21, 3389 packets, rumint v1.60)



SOTM 21, AMD2500+, 1GB RAM
all visualizations at 1280x1024 except
byte frequency and presences which are fixed at 256x418

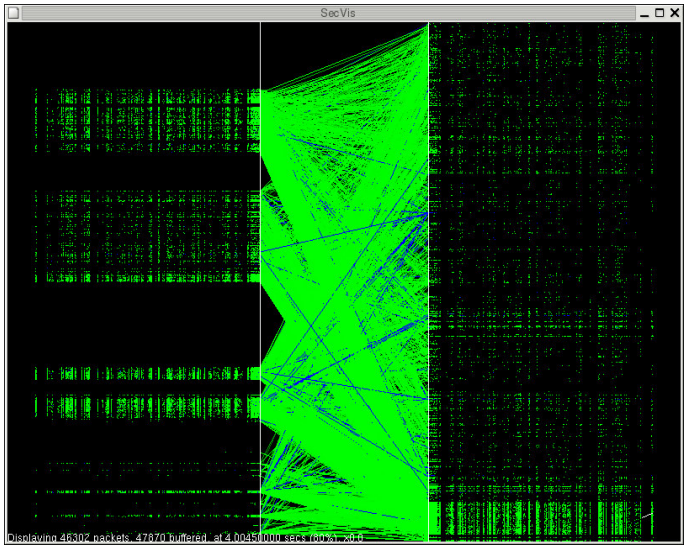
System Requirements

- IP over Ethernet
- Tested on Windows XP
- ~256+ MB Ram
- Processor 300MHZ (minimum)
- The more screen real estate the better
- Requires winpcap (I've used 3.0)

- Development
  - Visual Studio 6
  - port to GCC and Open GL
  - PacketX for now
    - Go direct to (win)pcap

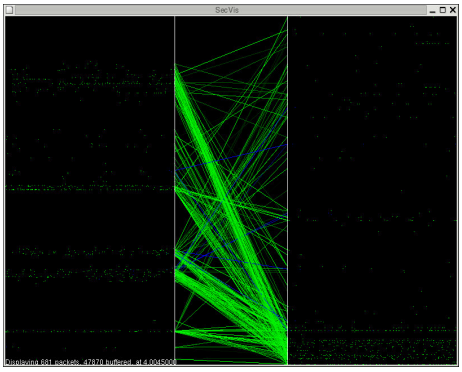
Inbound Campus Traffic

(5 seconds)

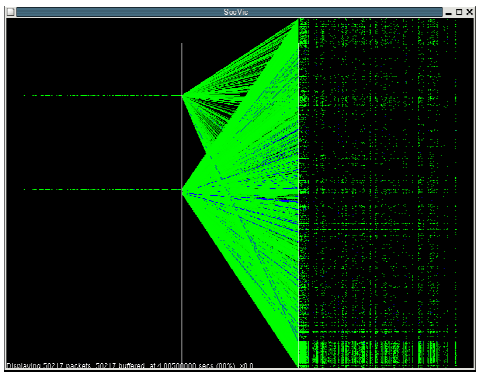


Campus Network Traffic

(10 msec capture)



inbound



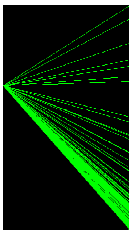
outbound

Directions for the Future…

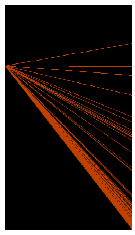
We are only scratching the surface of the possibilities

- **attack specific community needs**
- **plug-ins**
- launch network packets?
- **protocol specific visualizations**
  - including application layer (e.g. VoIP, HTTP)
- Open GL
- graph visualization+
- screensaver/wallpaper snapshot?
- work out GUI issues
- database of filters / smart books
- stress testing
- evaluate effectiveness

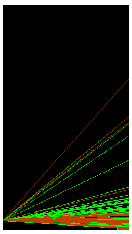
Library of Tool Fingerprints



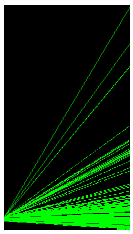
nmap 3 (RH8)



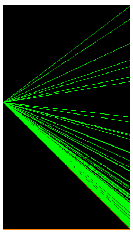
nmap 3 UDP (RH8)



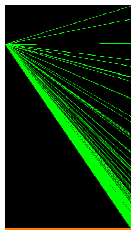
scanline 1.01 (XP)



SuperScan 3.0 (XP)

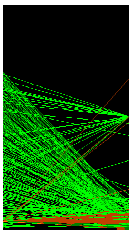


NMapWin 3 (XP)



nmap 3.5 (XP)

nikto 1.32 (XP)



SuperScan 4.0 (XP)

For more information…

G. Conti and K. Abdullah; " Passive Visual Fingerprinting of Network Attack Tools;" ACM Conference on Computer and Communications Security's Workshop on Visualization and Data Mining for Computer Security (VizSEC); October 2004.

--Talk PPT Slides

G. Conti; "Network Attack Visualization;" DEFCON 12; August 2004.

--Talk PPT Slides
--Classical InfoVis Survey PPT Slides
--Security InfoVis Survey PPT Slides

see www.cc.gatech.edu/~conti

Demo

Attacking the Analyst…

G. Conti, M. Ahamad and J. Stasko; "Attacking Information Visualization System Usability: Overloading and Deceiving the Human;" *Symposium on Usable Privacy and Security (SOUPS)*; July 2005. On the CD…

G. Conti and M. Ahamad; "A Taxonomy and Framework for Countering Denial of Information Attacks;" *IEEE Security and Privacy*. (accepted, to be published) Email me…

Attacking Information Visualization System Usability
Overloading and Deceiving the Human

Gregory Conti
College of Computing
Georgia Institute of Technology

Mustaque Ahamad
College of Computing
Georgia Institute of Technology

John Stasko
College of Computing
Georgia Institute of Technology

DEFCON CTF DoI vs. DOS…

On the CD…

- Talk slides (extended version)
- Code
  - rumint
  - secvis
  - rumint file conversion tool (pcap to rumint)
- Papers
  - SOUPS Malicious Visualization paper
  - Hacker conventions article
- Data
  - SOTM 21 .rum .pcap

See also: www.cc.gatech.edu/~conti and www.rumint.org

CACM

Feedback Requested…

- Tasks
- Usage
  - provide feedback on GUI
  - needed improvements
  - multiple monitor machines
  - performance under stress
  - bug reports
- Data
  - interesting packet traces
  - screenshots
    - with supporting .rum and .pcap files, if possible
- Pointers to interesting related tools (viz or not)
- New viz and other analysis ideas

Volunteers to participate in user study

Acknowledgements

404.se2600, Kulsoom Abdullah, Sandip Agarwala, Mustaque Ahamad, Bill Cheswick, Chad, Clint, Tom Cross, David Dagon, DEFCON, Ron Dodge, EliO, Emma, Mr. Fuzzy, Jeff Gribschaw, Julian Grizzard, GTISC, Hacker Japan, Mike Hamelin, Hendrick, Honeynet Project, Interz0ne, Jinsuk Jun, Kenshoto, Oleg Kolesnikov, Sven Krasser, Chris Lee, Wenke Lee, John Levine, Michael Lynn, David Maynor, Neel Mehta, Jeff Moss, NETI@home, Henry Owen, Dan Ragsdale, Rockit, Byung-Uk Roho, Charles Robert Simpson, Ashish Soni, SOUPS, Jason Spence, John Stasko, StricK, Susan, USMA ITOC, IEEE IAW, VizSEC 2004, Grant Wagner and the Yak.

- 100+ Graduate Level InfoSec Researchers
- Multiple InfoSec degree and certificate programs

- Representative Research
  - User-centric Security
  - Adaptive Intrusion Detection Models
  - Defensive Measures Against Network Denial of Service Attacks
  - Exploring the Power of Safe Areas of Computation
  - Denial of Information Attacks (Semantic Hacking)
  - Enterprise Information Security

- **Looking for new strategic partners, particularly in industry and government**

www.gtisc.gatech.edu

Questions?

Greg Conti
conti@cc.gatech.edu

www.cc.gatech.edu/~conti
www.rumint.org

Image: http://altura.speedera.net/ccimg.catalogcity.com/210000/211700/211780/Products/6203927.jpg