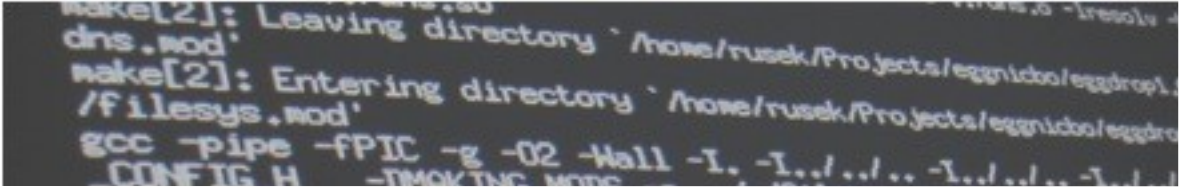


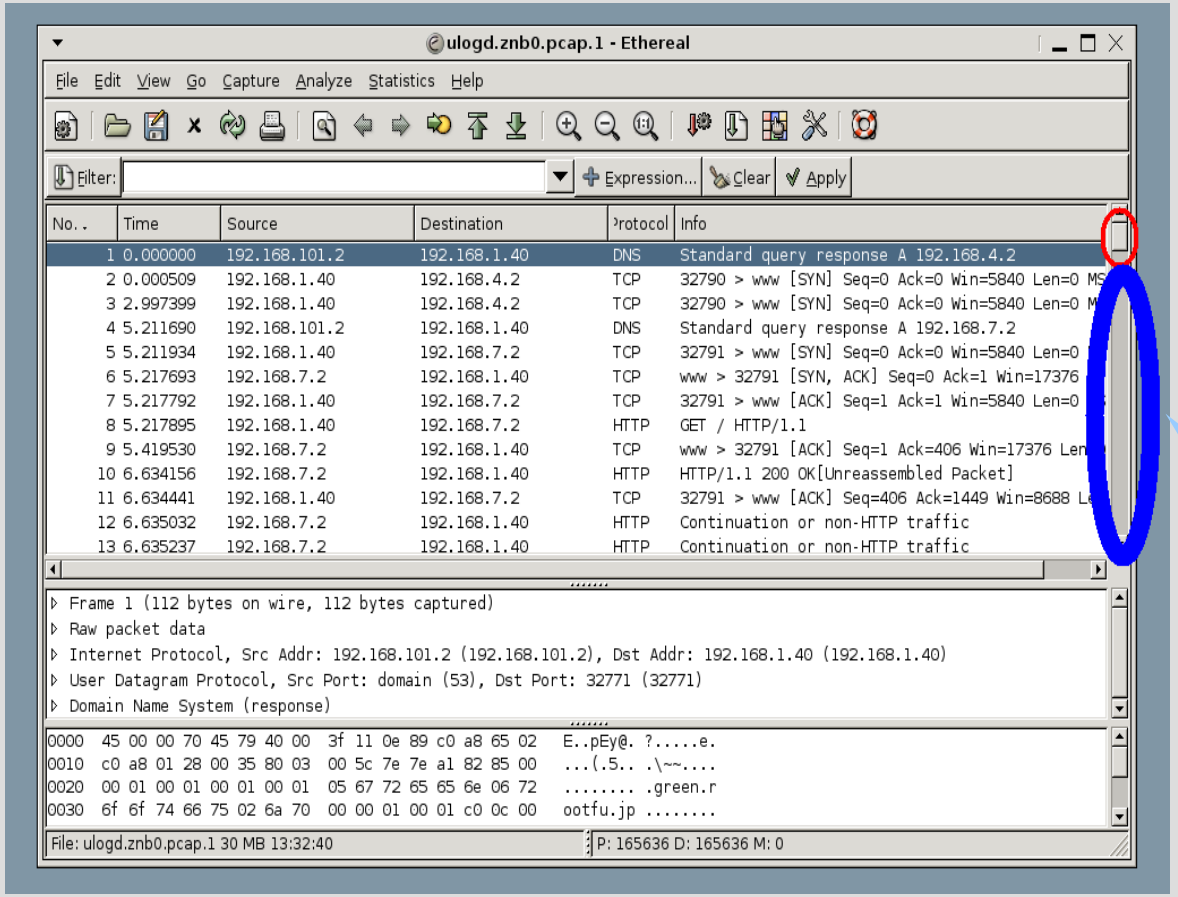
Backhoe: a packet trace & log browser

Sergey Bratus
Axel Hansen
Fabio Pellacini
Anna Shubina

Dartmouth College
INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
Cyber Security and Trust Research & Development
http://www.ISTS.dartmouth.edu

Motivation

Network analysis tools give no clue of what lies beyond the current “window”.



Can we:

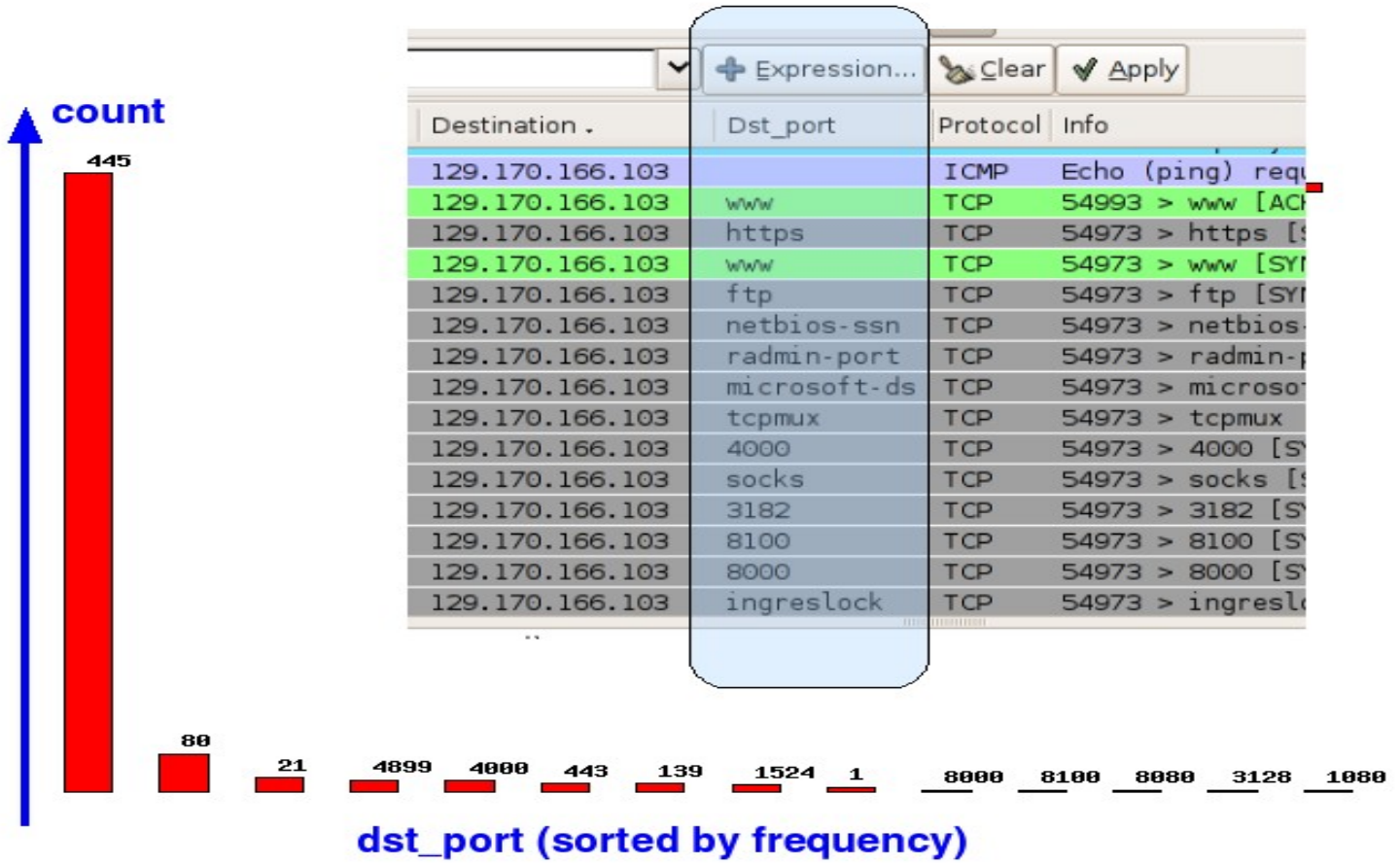
- drill down to packets &
- provide a visual summary?

Uncertainty

Measure uncertainty...

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES

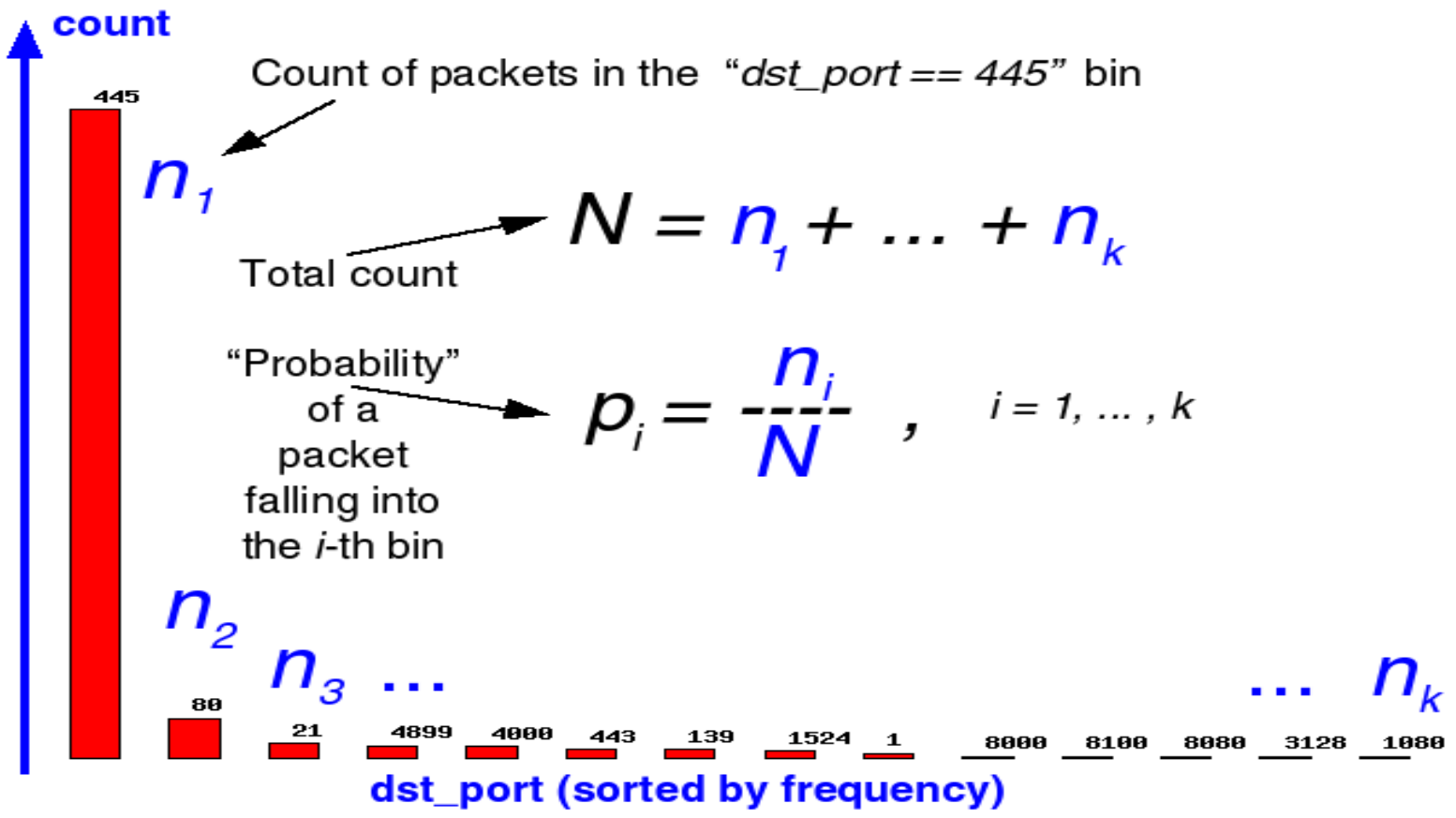
as entropy of field value frequency distributions



Entropy reminder

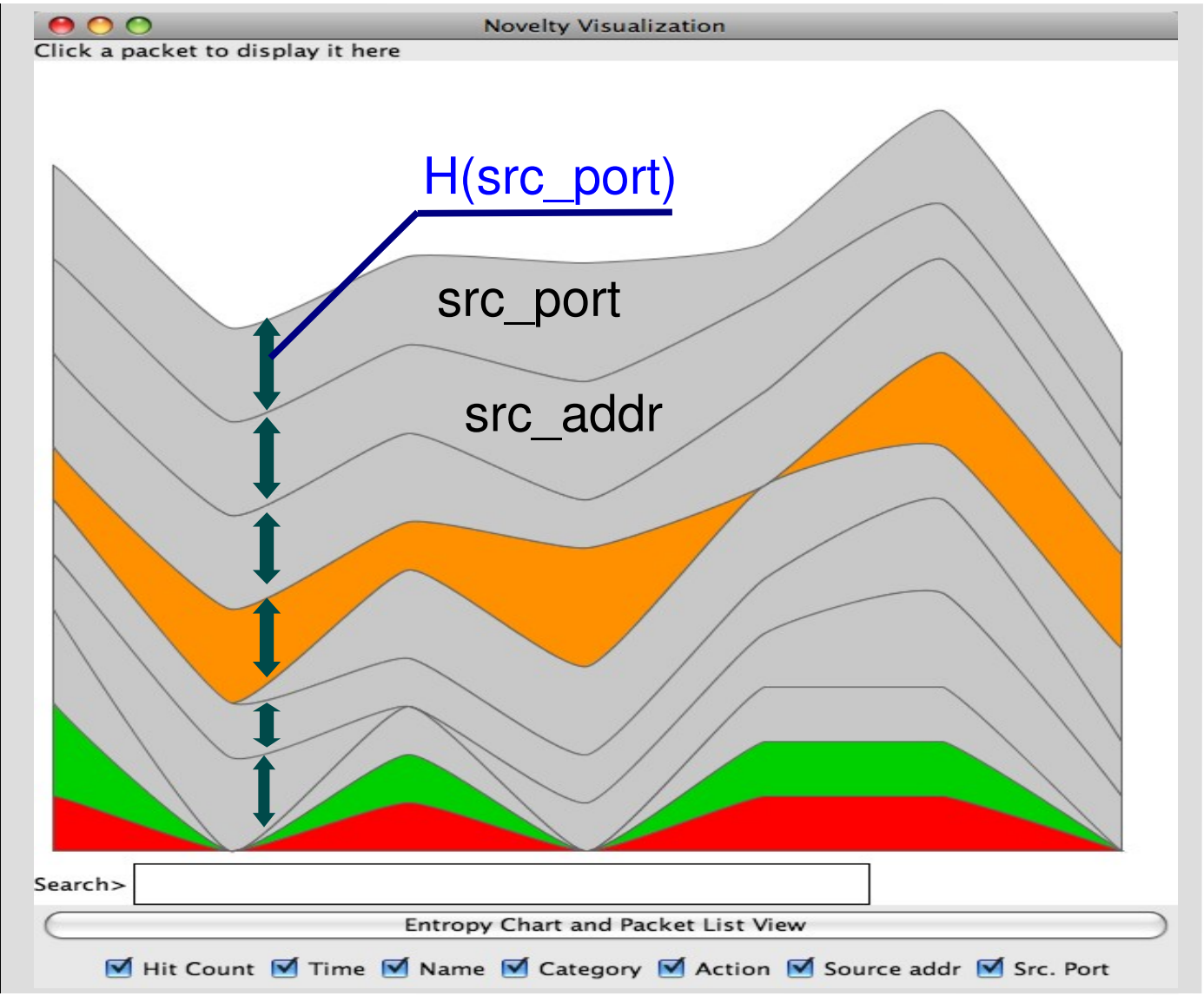
Entropy of a discrete distribution:

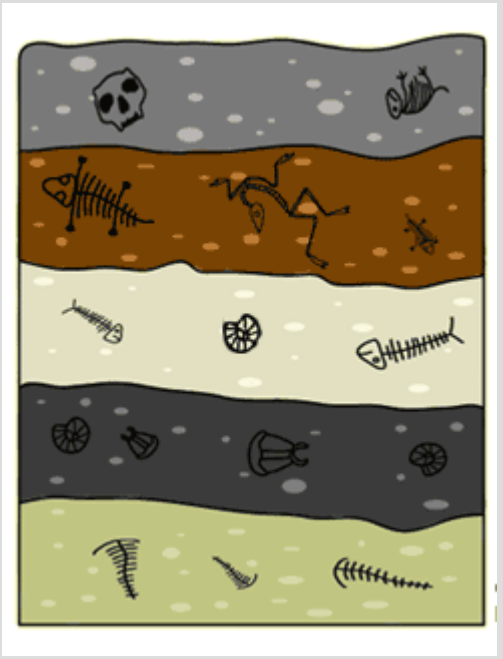
$$H(X) = \sum_{i=1}^{k} p_i \cdot \log_2 \frac{1}{p_i}$$



Backhoe: the "Strata" view

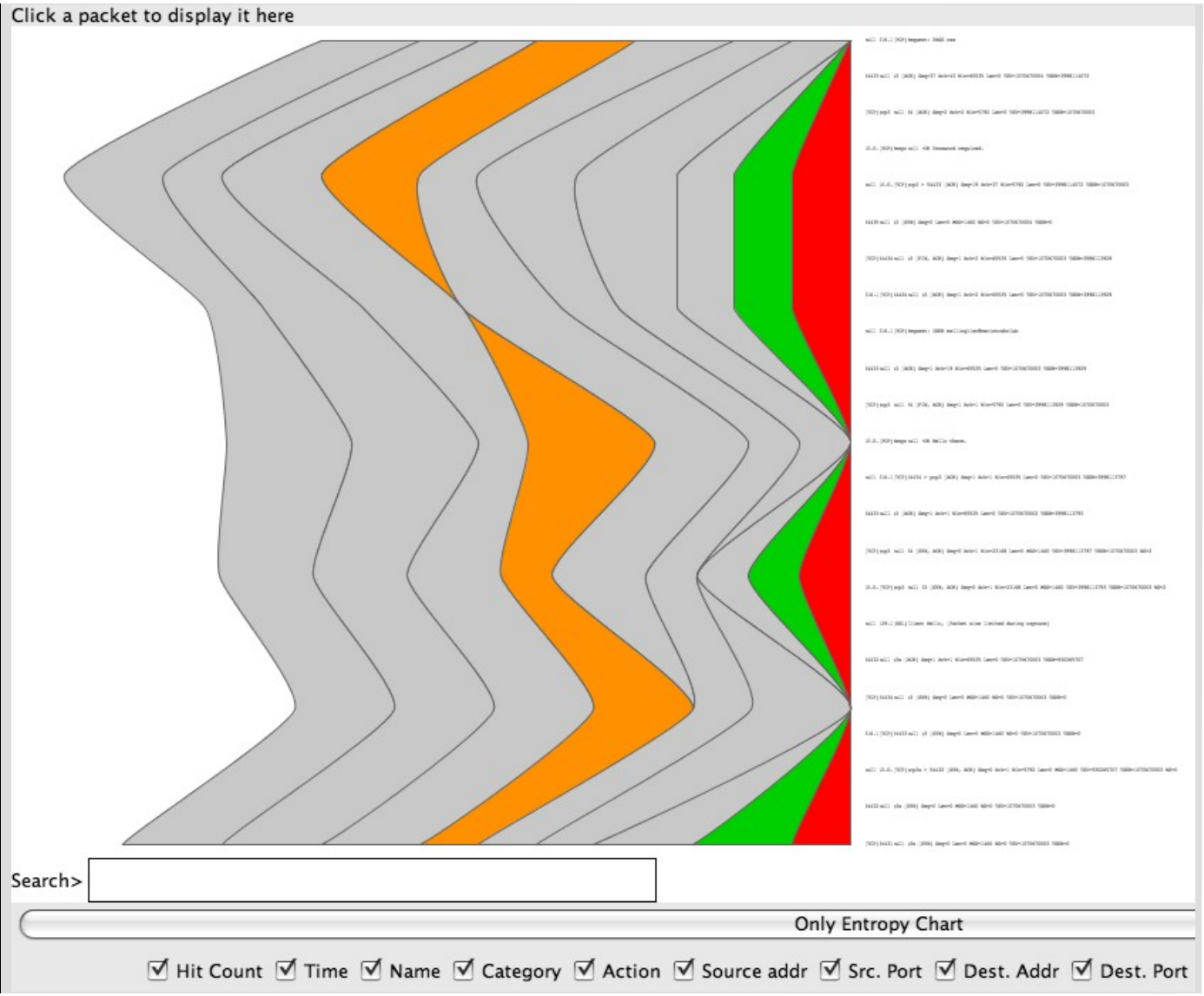
Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES

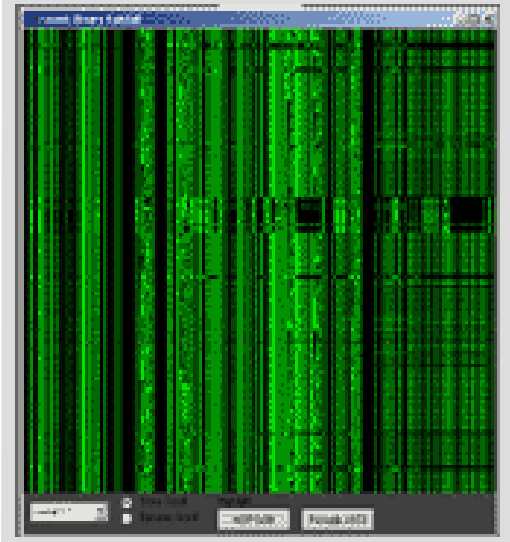




“Packet fall” view

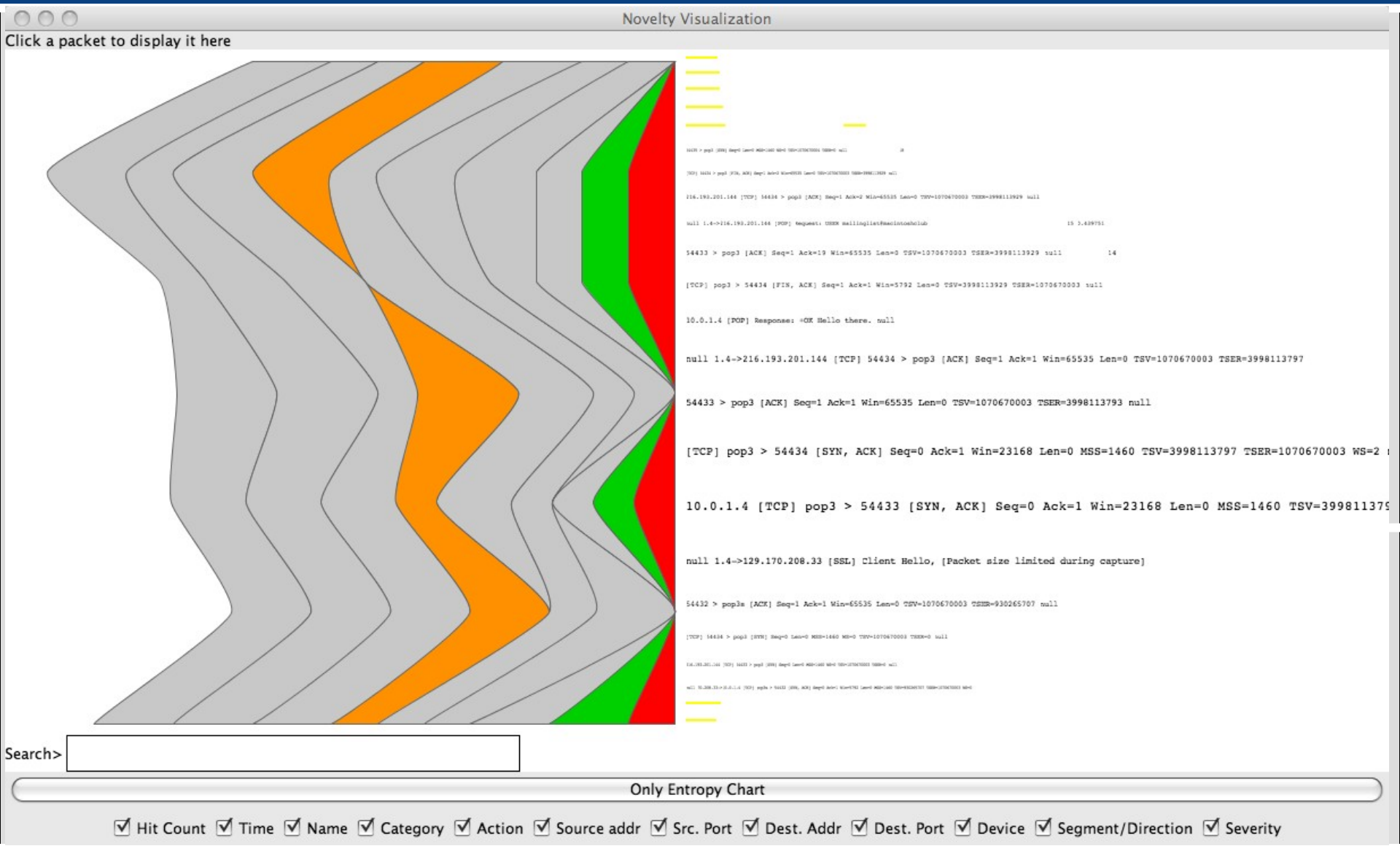
Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES





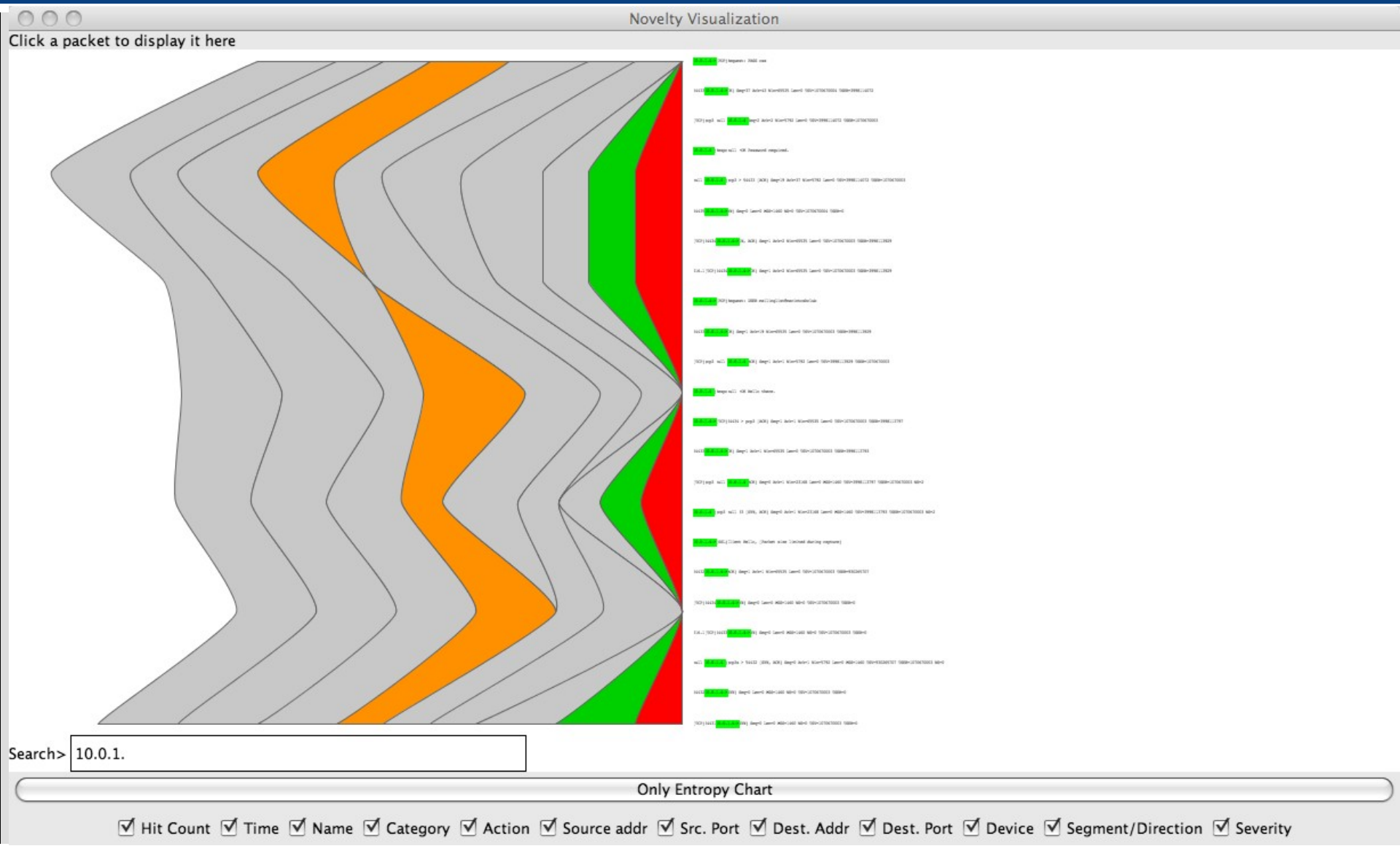
“Packet fall” + fish eye

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES



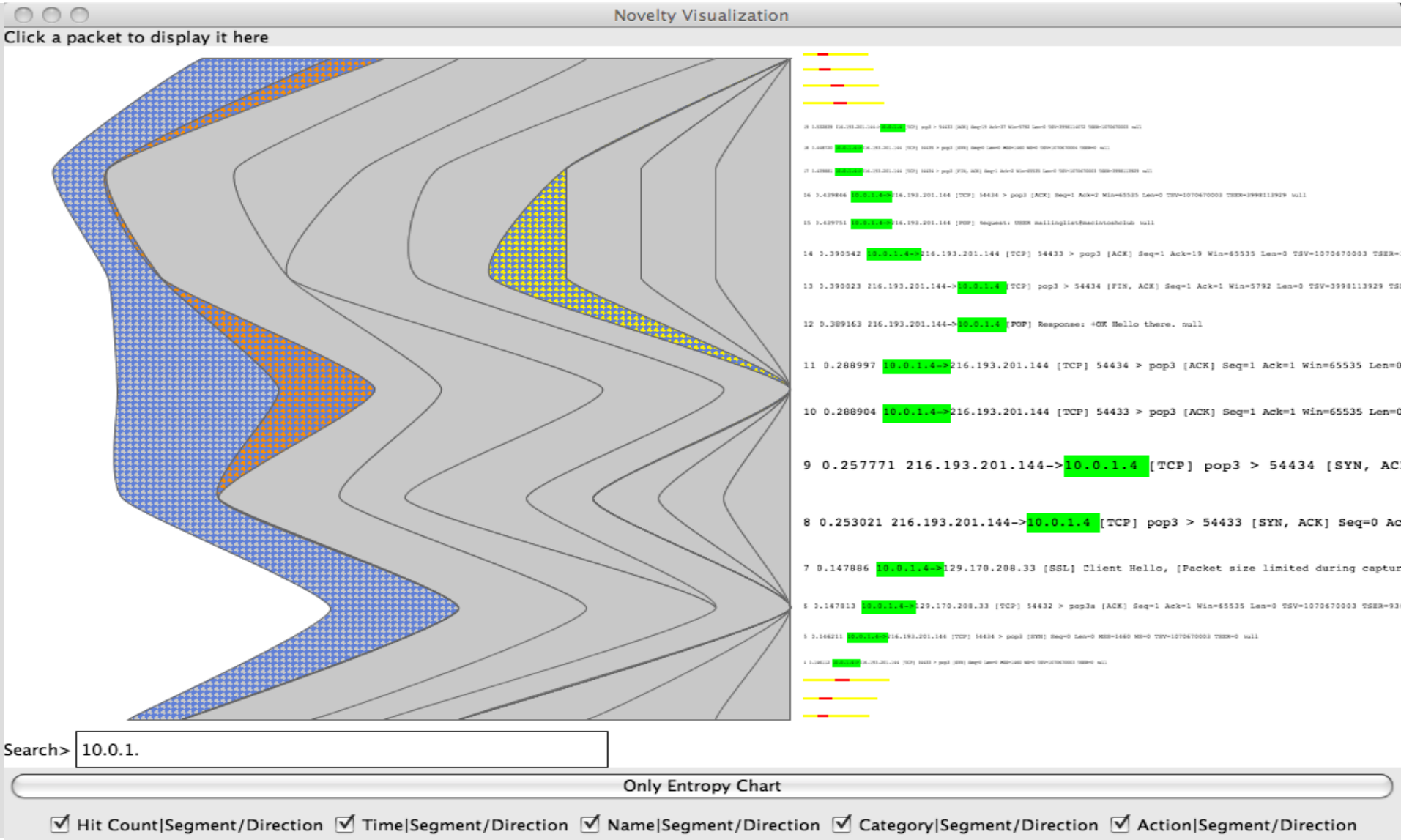
“Packet fall” + search

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES



Search + fish eye

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES

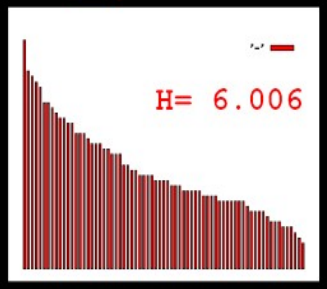


Joint and conditional entropy

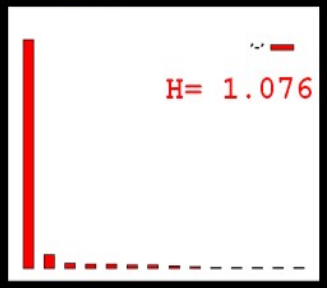
Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES

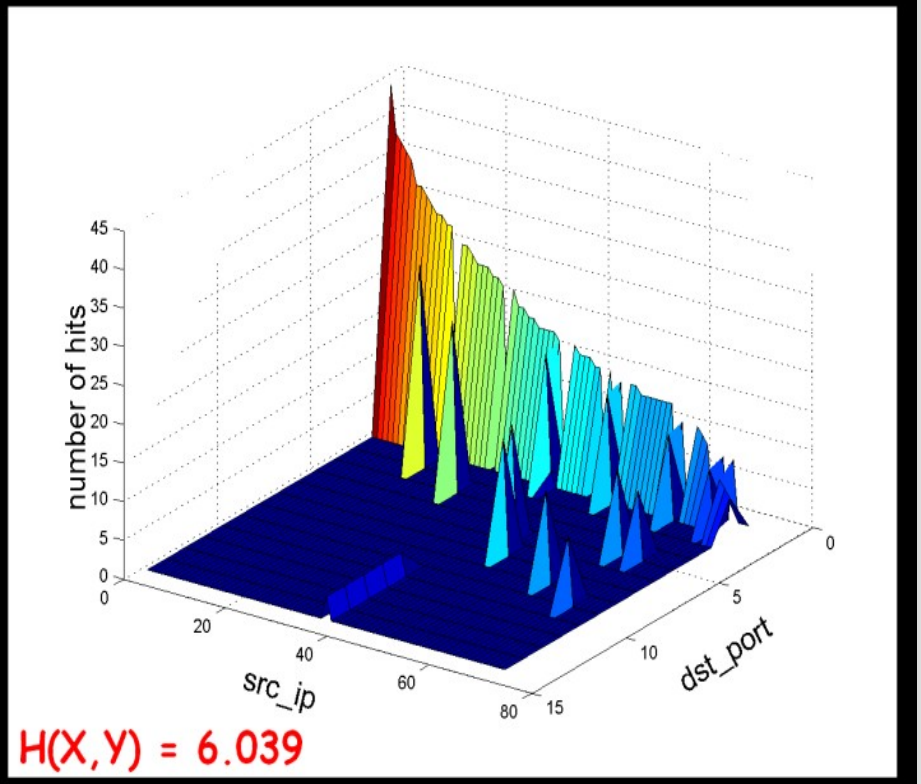
$$H(X, Y) <= H(X) + H(Y)$$

src_ip

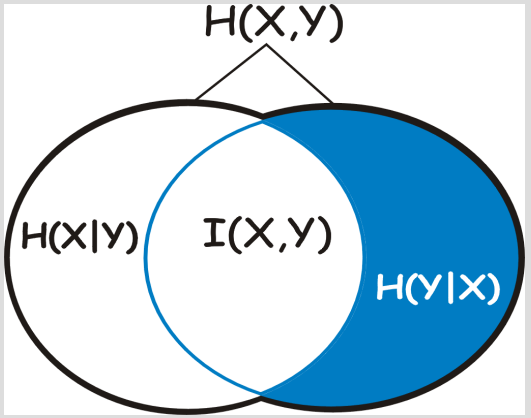


dst_port

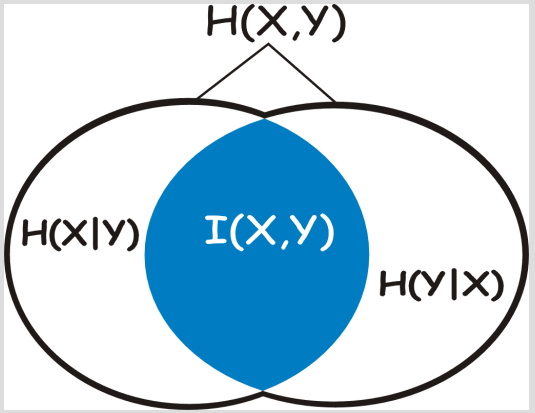




$$I(X; Y) := H(X) + H(Y) - H(X, Y)$$



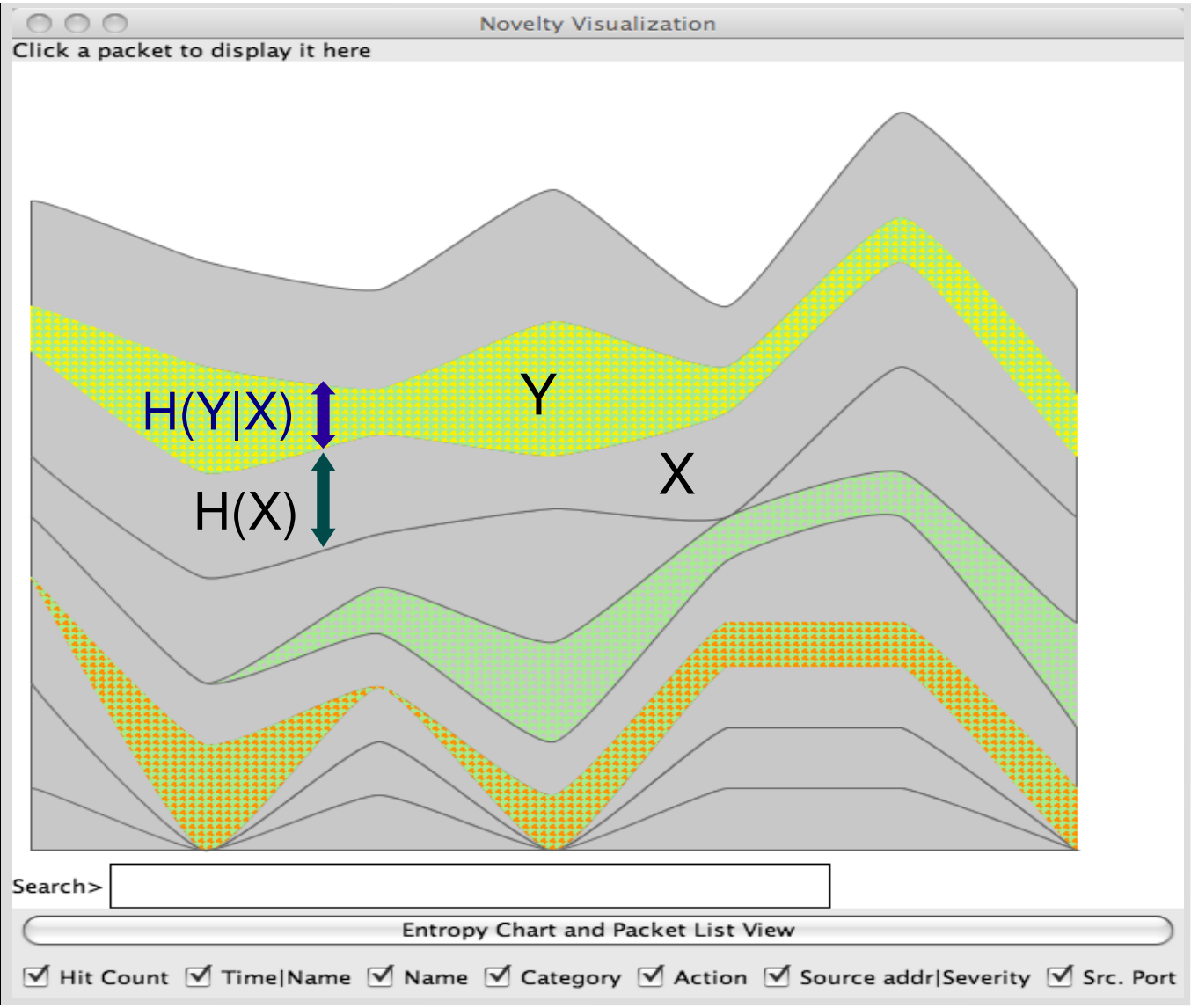
Conditional entropy

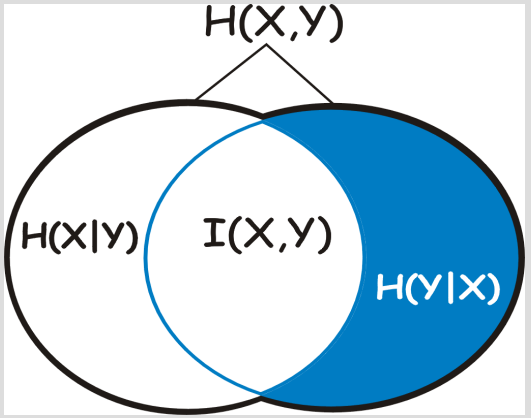


Mutual information

Joint and conditional entropy

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES



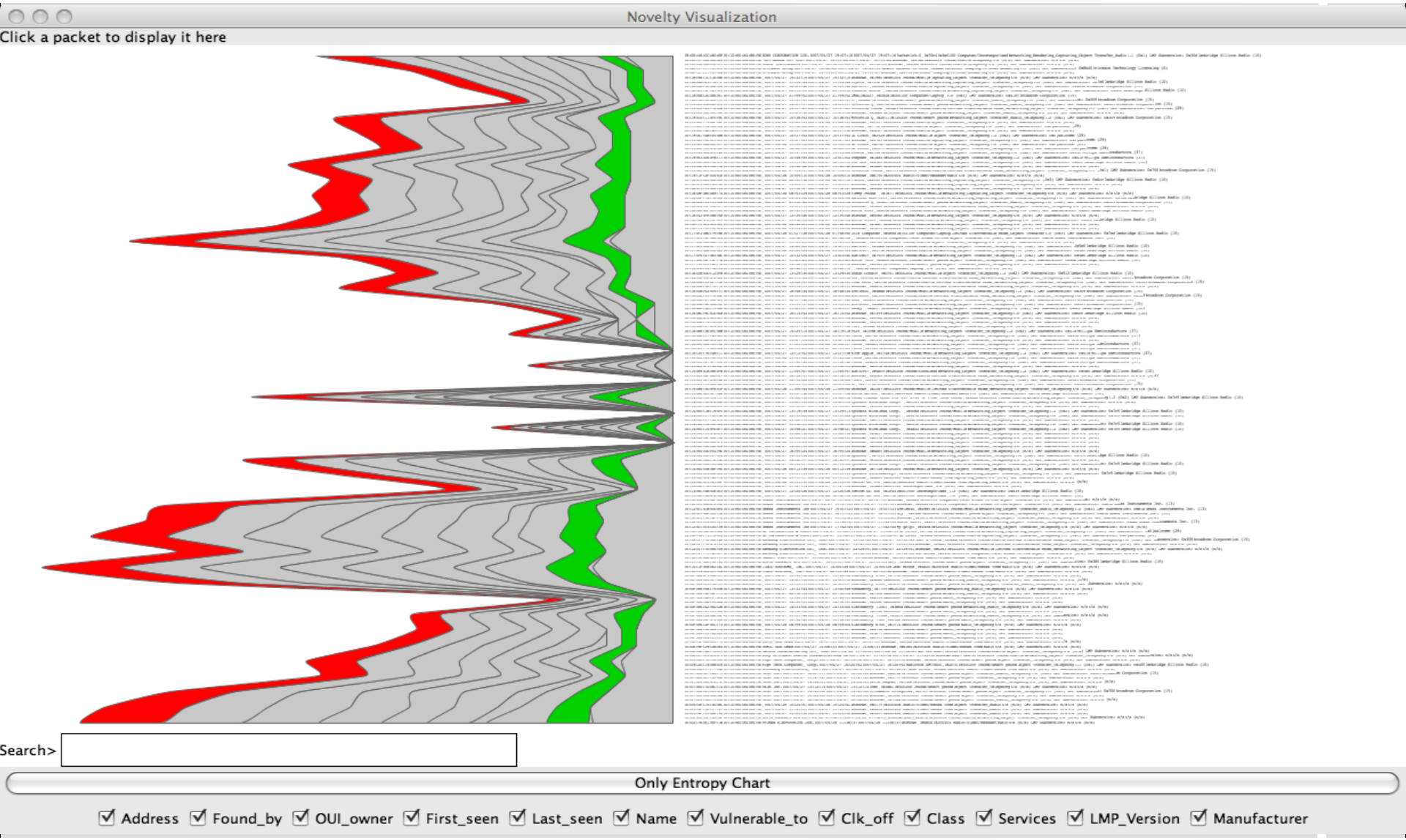


$H(Y|X)=H(X,Y) - H(X)$

H(Y|X) shows how much uncertainty remains about Y once we know X

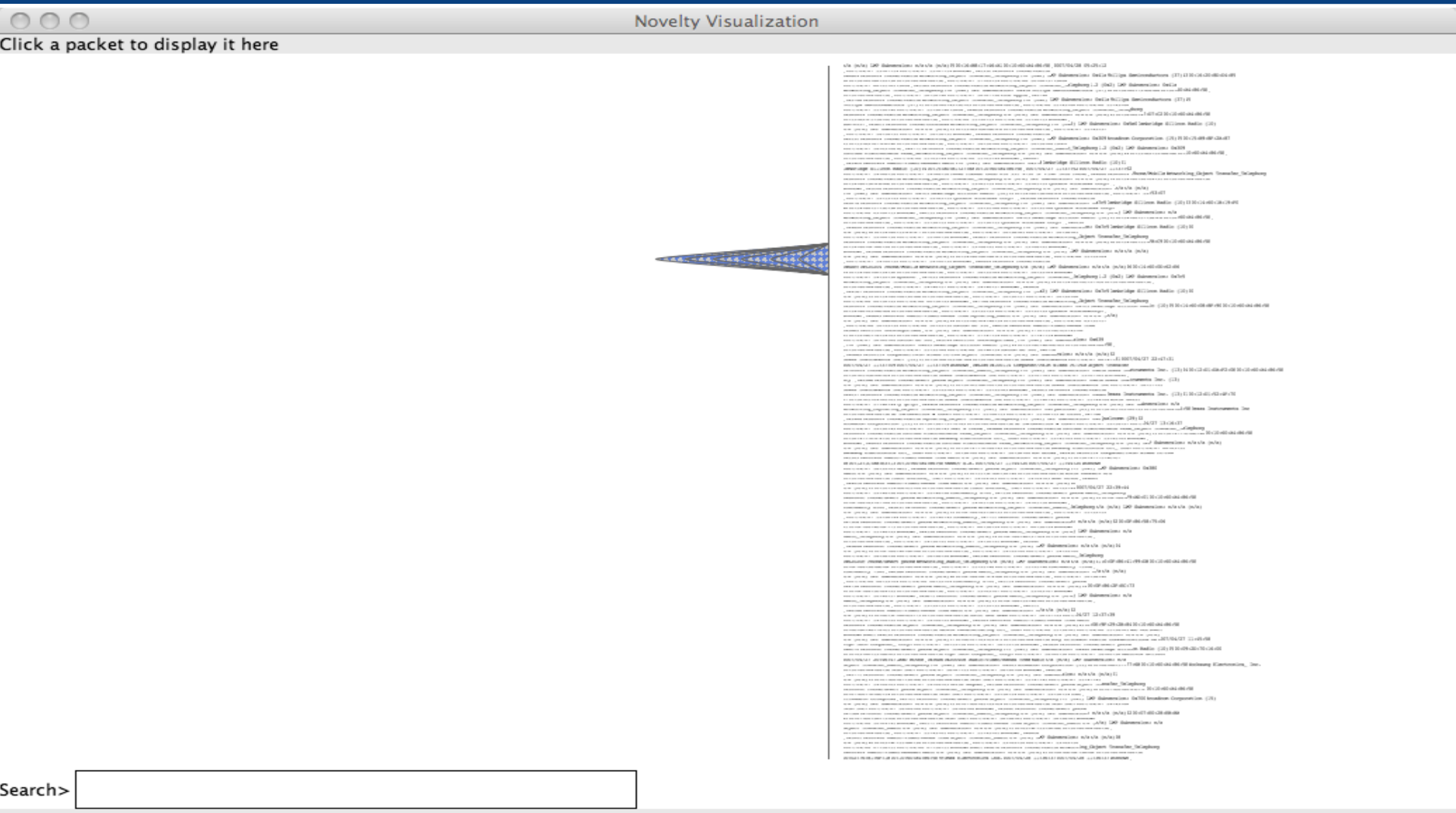
Use case: “Bluesnarfing”

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES



Bluesnarfing, conditioned

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES



Source & Thanks

Dartmouth College
INSTITUTE FOR SECURITY
TECHNOLOGY STUDIES

http://kerf.cs.dartmouth.edu/backhoe/

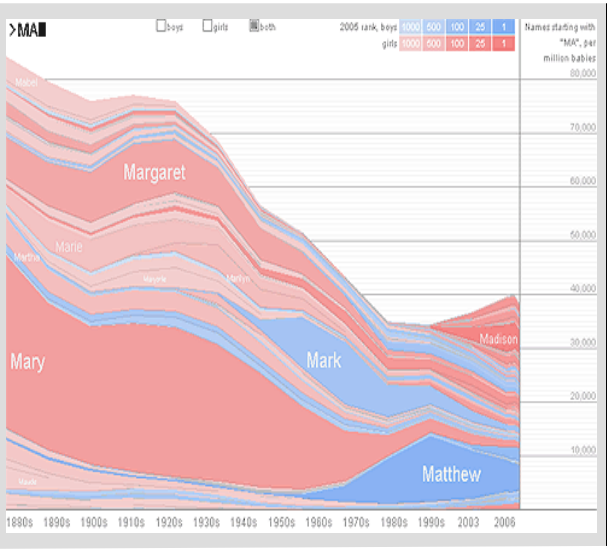
- Java sources will be posted soon

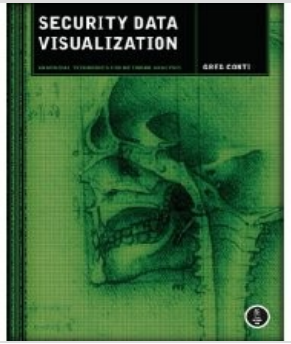
Thanks:

- Jeffrey Heer, *Prefuse* (*prefuse.org*)
- Martin Wattenberg, *NameVoyager*

- Greg Conti, *Rumint* and other security visualisation tools

prefuse





Contact Information

Institute for Security Technology Studies
Dartmouth College
6211 Sudikoff Laboratory
Hanover, NH 03755

Phone: 603.646.0700
Fax: 603.646.1672

Email: info@ists.dartmouth.edu