

```
make[2]: Leaving directory ` /home/rusek/Projects/eggnidool/eggdrops  
dns.mod'  
make[2]: Entering directory ` /home/rusek/Projects/eggnidool/eggdrops  
/filesys.mod'  
gcc -pipe -fPIC -g -O2 -Wall -I. -I../.. -I../.. -I.. -I..  
CONFIG_H -DMODING MODE
```

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”.

The screenshot shows the Wireshark interface with a list of 13 captured packets. The selected packet (No. 1) is a DNS standard query response. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.101.2	192.168.1.40	DNS	Standard query response A 192.168.4.2
2	0.000509	192.168.1.40	192.168.4.2	TCP	32790 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 M...
3	2.997399	192.168.1.40	192.168.4.2	TCP	32790 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 M...
4	5.211690	192.168.101.2	192.168.1.40	DNS	Standard query response A 192.168.7.2
5	5.211934	192.168.1.40	192.168.7.2	TCP	32791 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 M...
6	5.217693	192.168.7.2	192.168.1.40	TCP	www > 32791 [SYN, ACK] Seq=0 Ack=1 Win=17376 L...
7	5.217792	192.168.1.40	192.168.7.2	TCP	32791 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 M...
8	5.217895	192.168.1.40	192.168.7.2	HTTP	GET / HTTP/1.1
9	5.419530	192.168.7.2	192.168.1.40	TCP	www > 32791 [ACK] Seq=1 Ack=406 Win=17376 Len=...
10	6.634156	192.168.7.2	192.168.1.40	HTTP	HTTP/1.1 200 OK[Unreassembled Packet]
11	6.634441	192.168.1.40	192.168.7.2	TCP	32791 > www [ACK] Seq=406 Ack=1449 Win=8688 L...
12	6.635032	192.168.7.2	192.168.1.40	HTTP	Continuation or non-HTTP traffic
13	6.635237	192.168.7.2	192.168.1.40	HTTP	Continuation or non-HTTP traffic

The detailed view of the selected packet shows the following structure:

- Frame 1 (112 bytes on wire, 112 bytes captured)
- Raw packet data
- Internet Protocol, Src Addr: 192.168.101.2 (192.168.101.2), Dst Addr: 192.168.1.40 (192.168.1.40)
- User Datagram Protocol, Src Port: domain (53), Dst Port: 32771 (32771)
- Domain Name System (response)

The hex dump and ASCII representation of the packet data are shown below:

```
0000 45 00 00 70 45 79 40 00 3f 11 0e 89 c0 a8 65 02  E..pEy@. ?.....e.
0010 c0 a8 01 28 00 35 80 03 00 5c 7e 7e a1 82 85 00  ...(.5.. \~~....
0020 00 01 00 01 00 01 00 01 05 67 72 65 65 6e 06 72  .....green.r
0030 6f 6f 74 66 75 02 6a 70 00 00 01 00 01 c0 0c 00  ootfu.jp .....
```

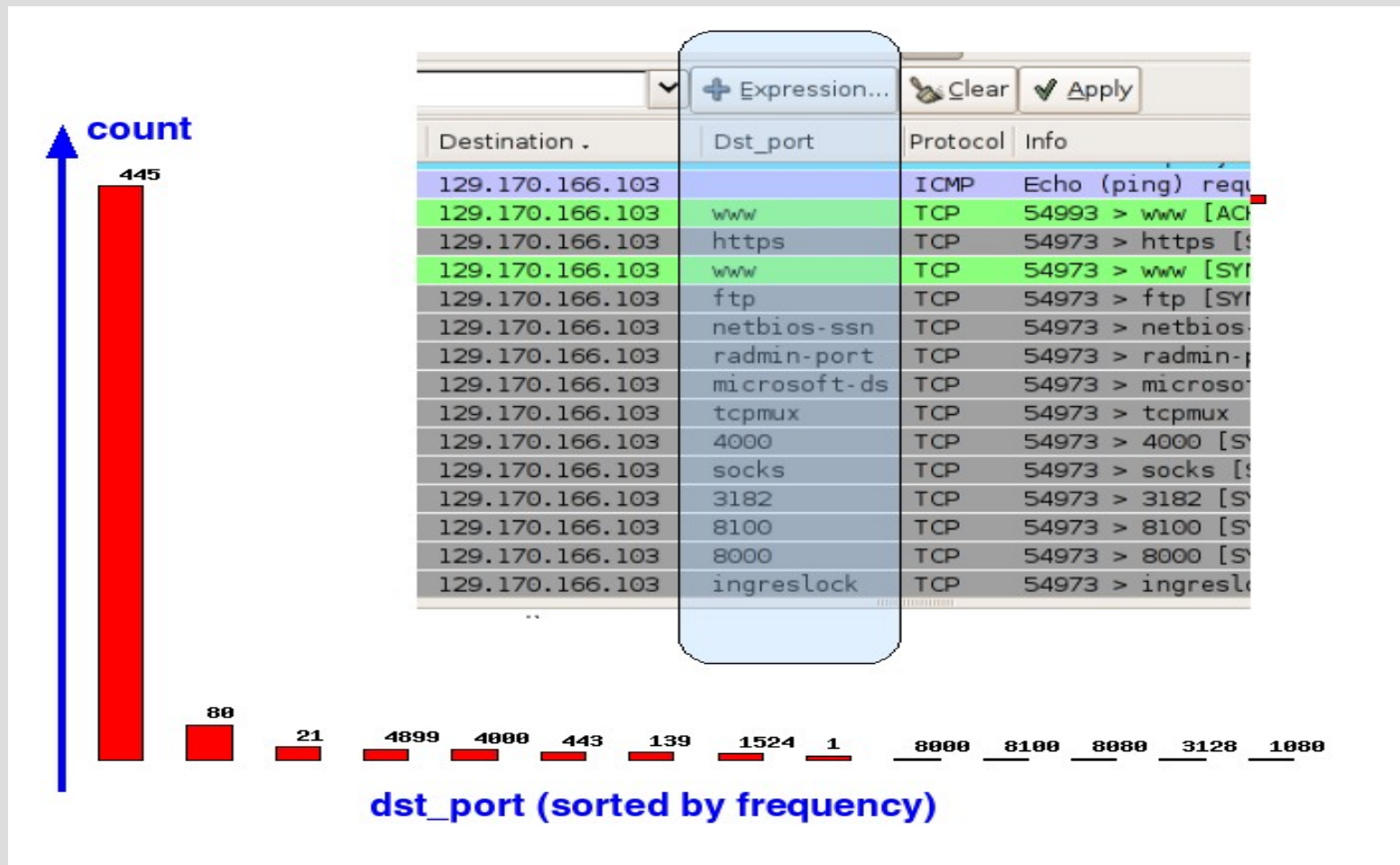
Can we:

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

Uncertainty

Measure uncertainty...

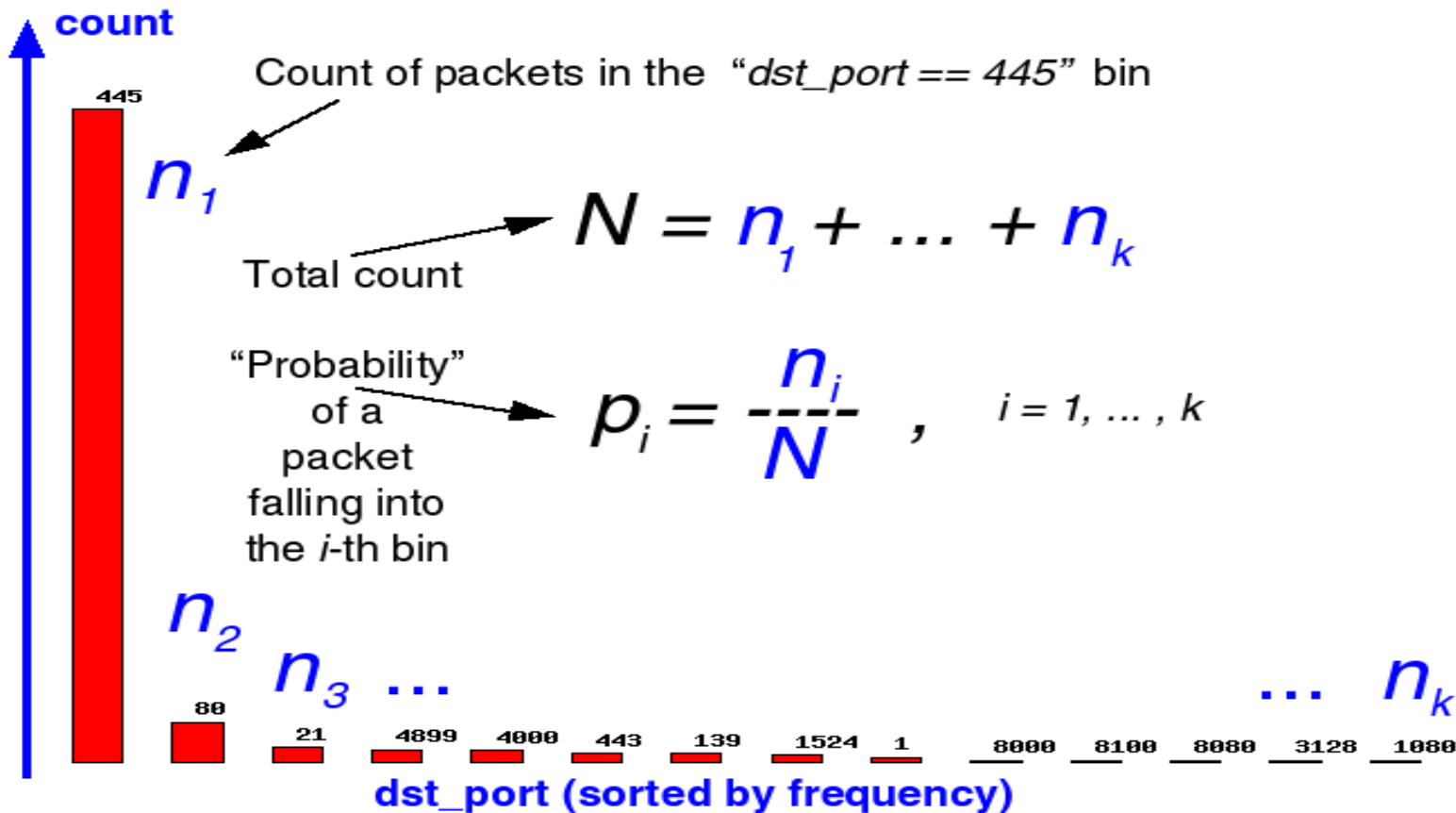
as **entropy** of field value frequency distributions



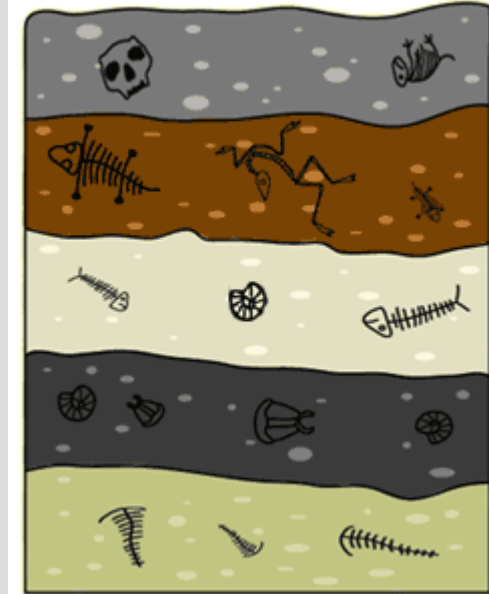
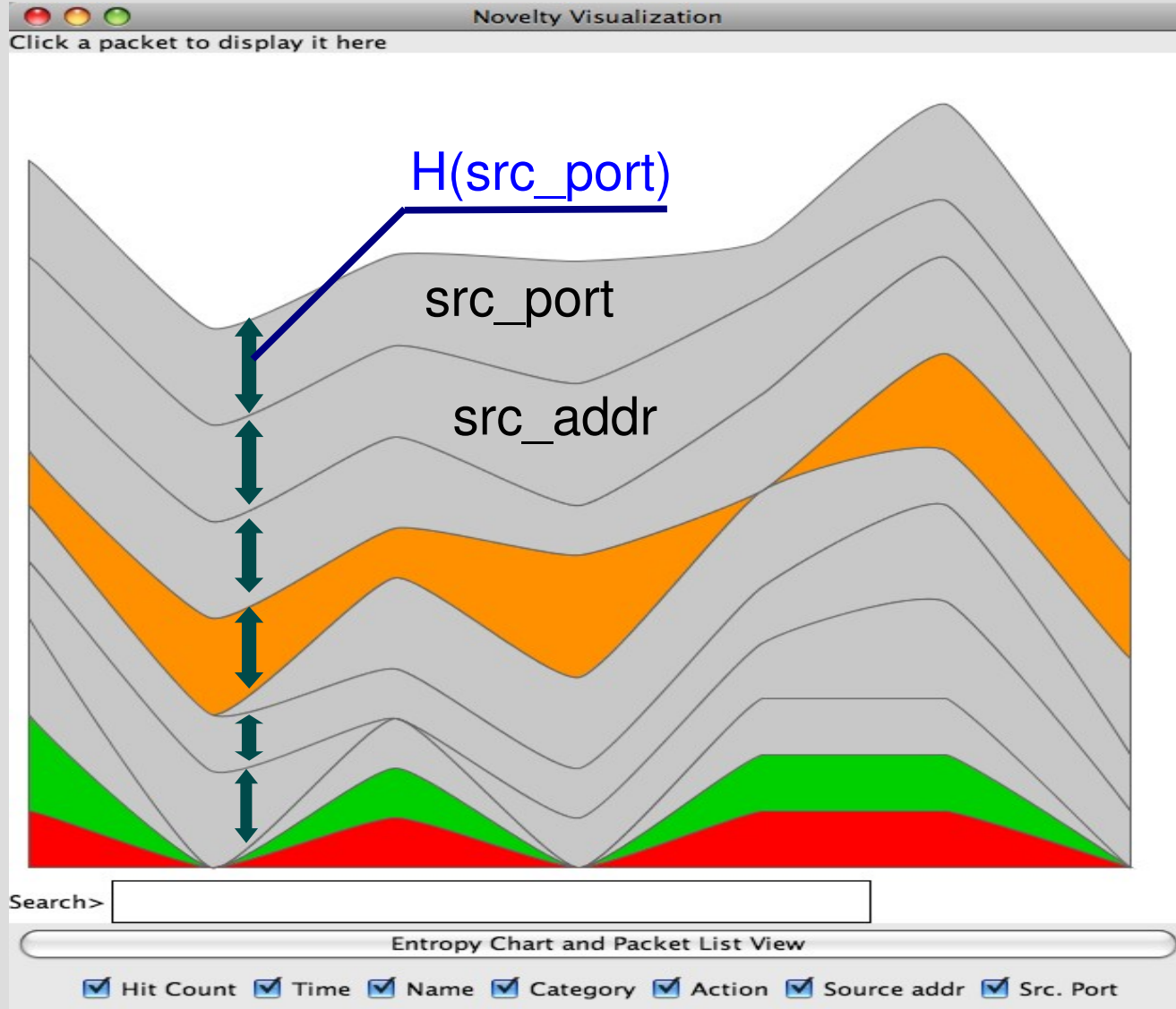
Entropy reminder

Entropy of a discrete distribution:

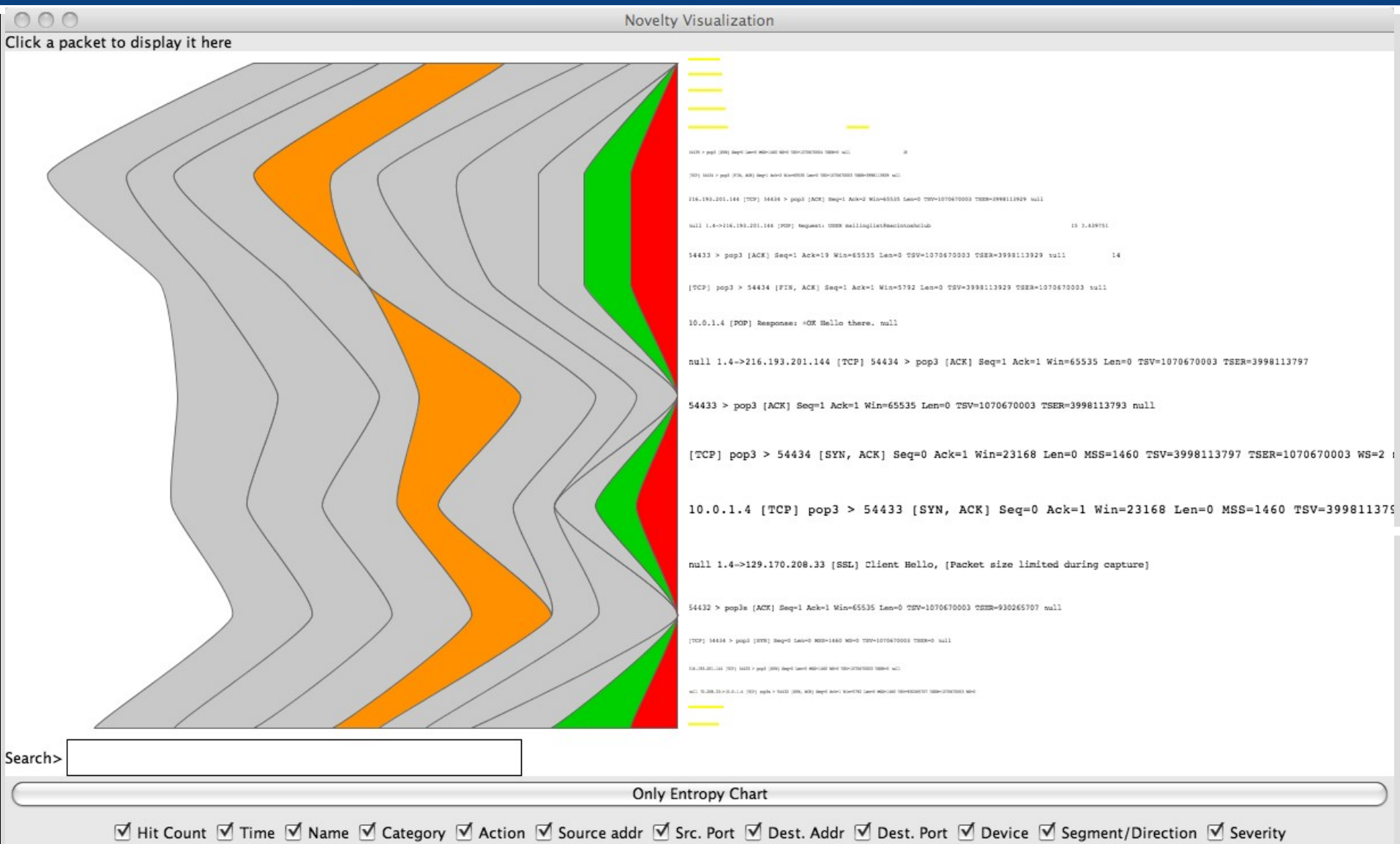
$$H(X) = \sum_{i=1}^k p_i \cdot \log_2 \frac{1}{p_i}$$



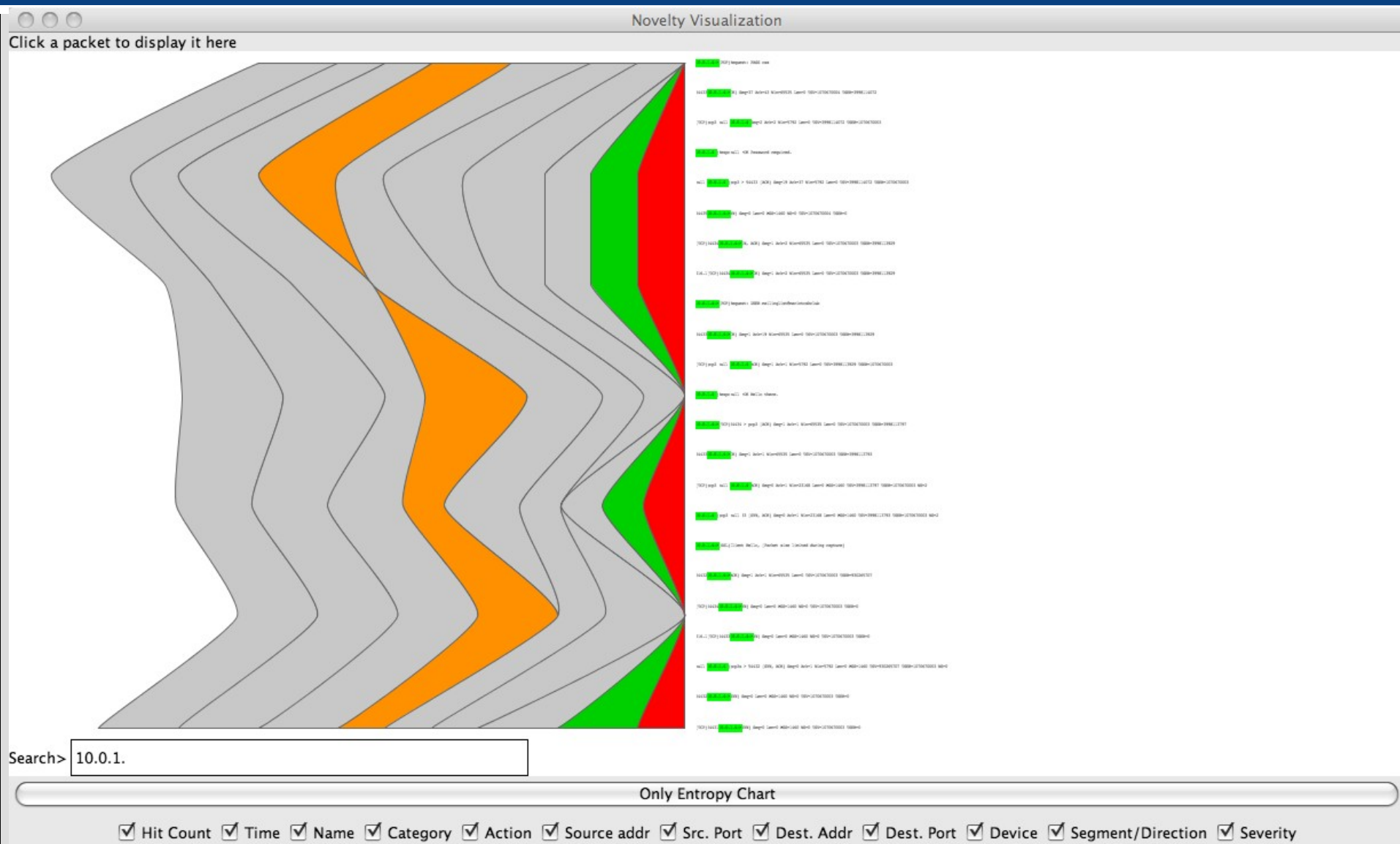
Backhoe: the "Strata" view



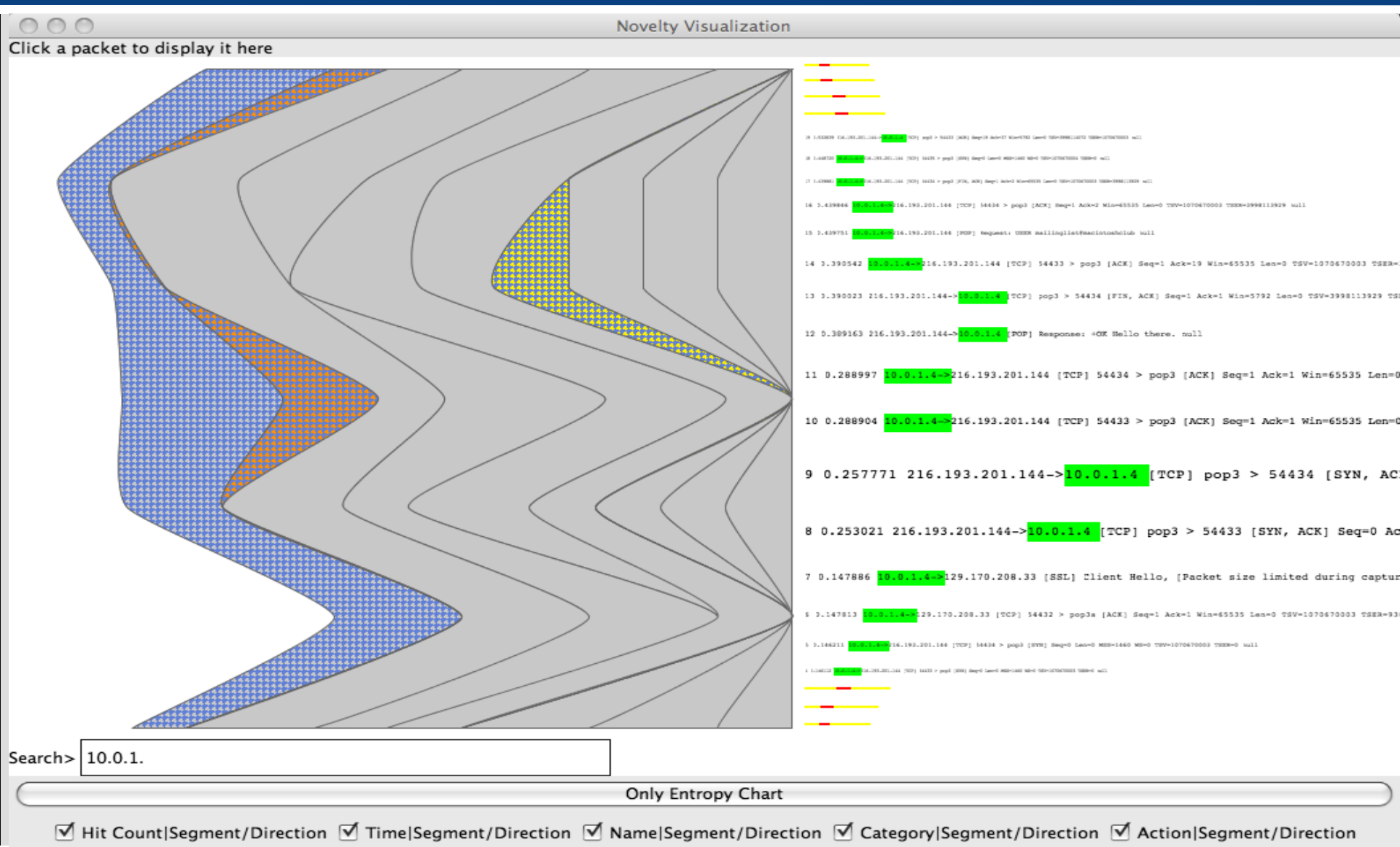
“Packet fall” + fish eye



“Packet fall” + search



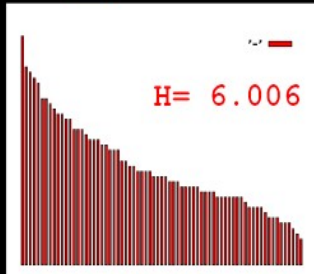
Search + fish eye



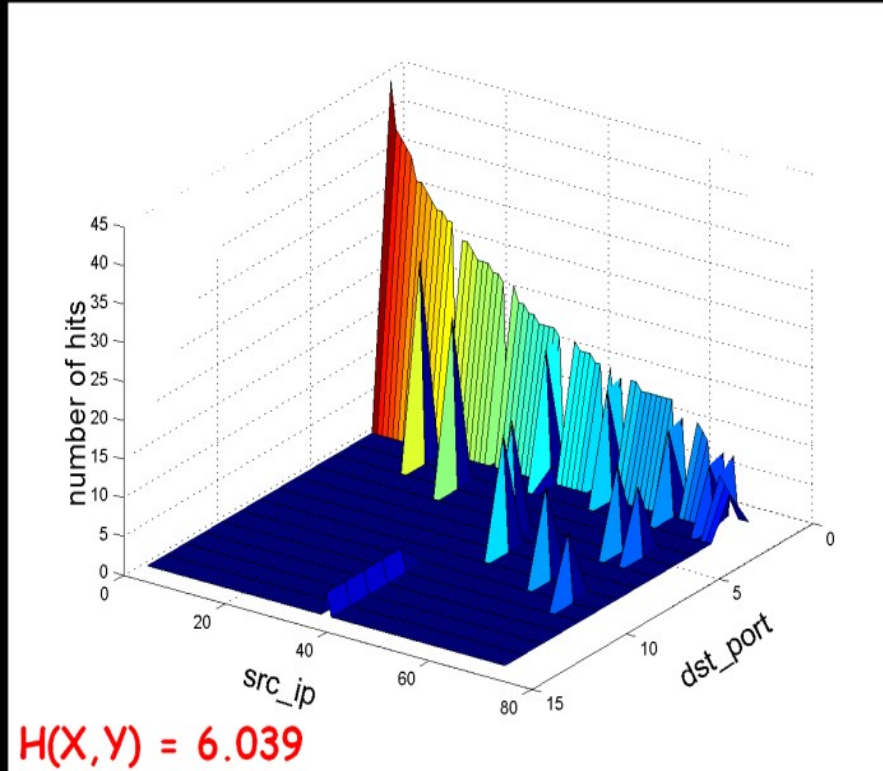
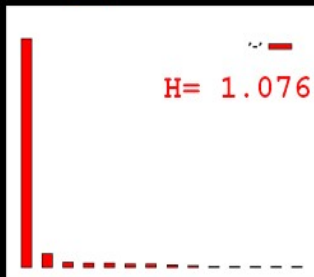
Joint and conditional entropy

$$H(X, Y) \leq H(X) + H(Y)$$

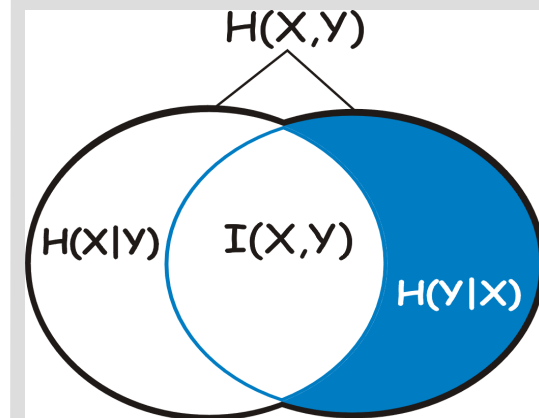
src_ip



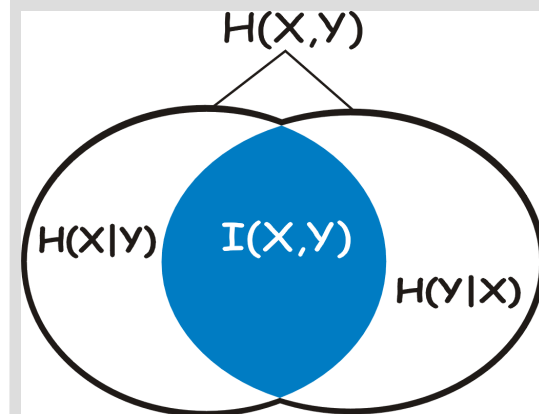
dst_port



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

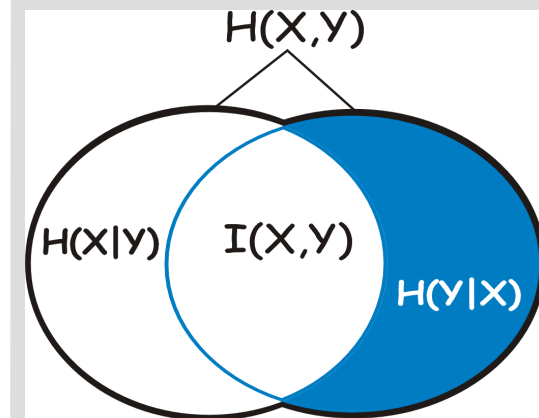
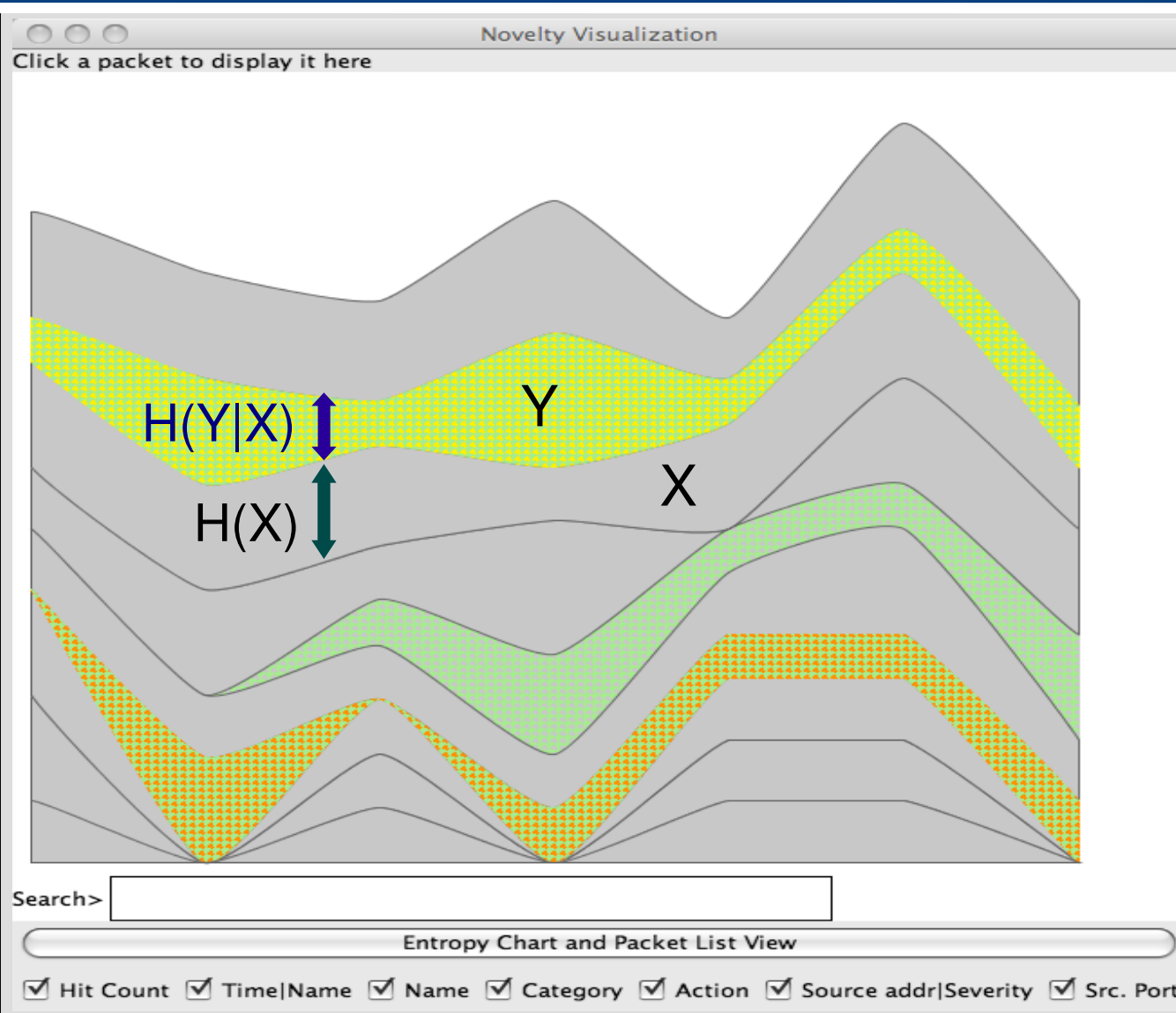


Conditional entropy



Mutual information

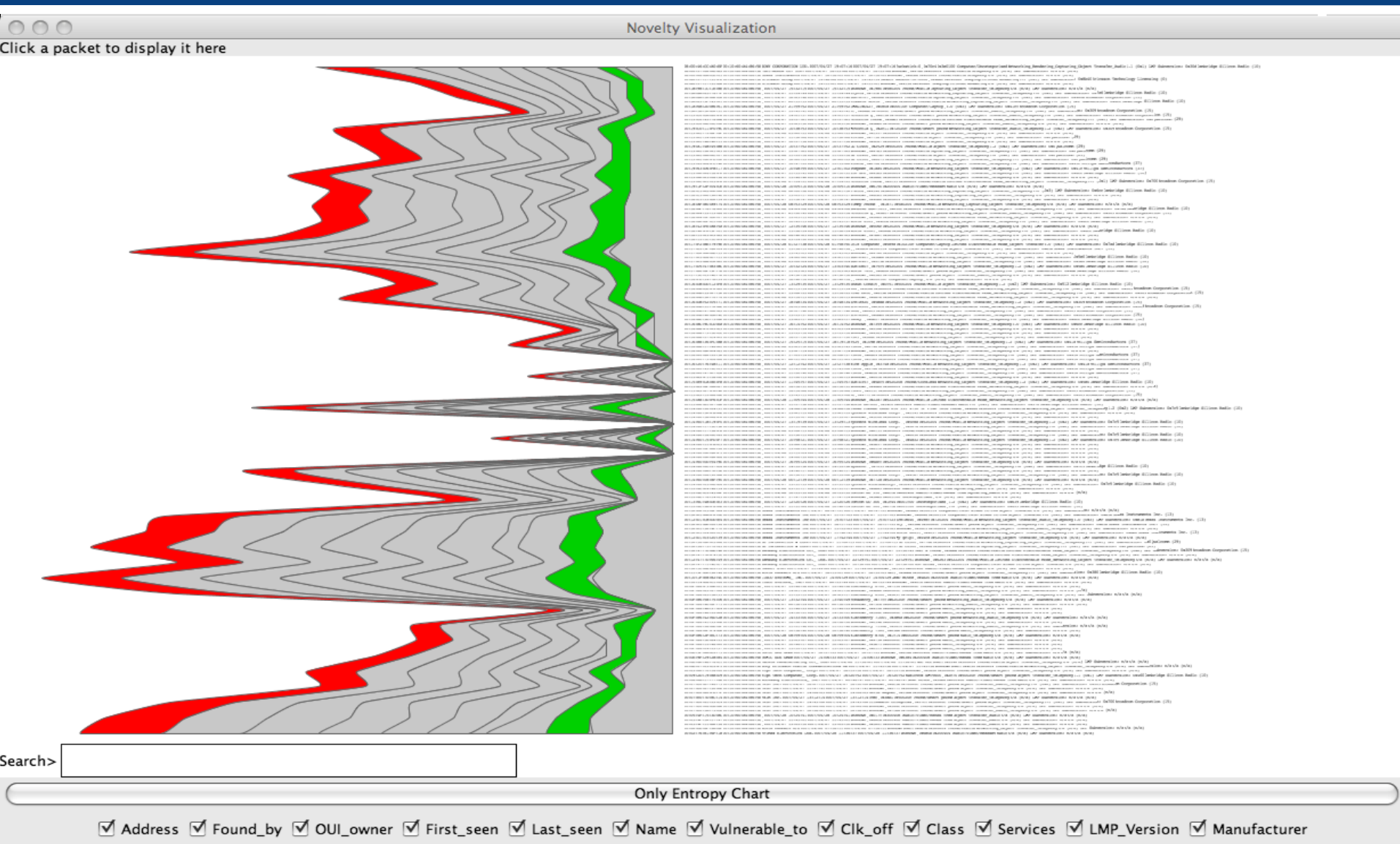
Joint and conditional entropy



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

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

Use case: "Bluesnarfing"



Source & Thanks

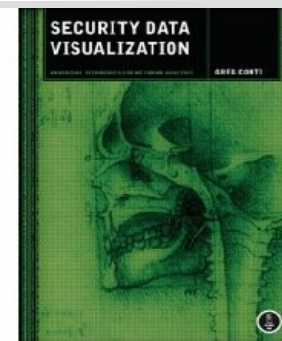
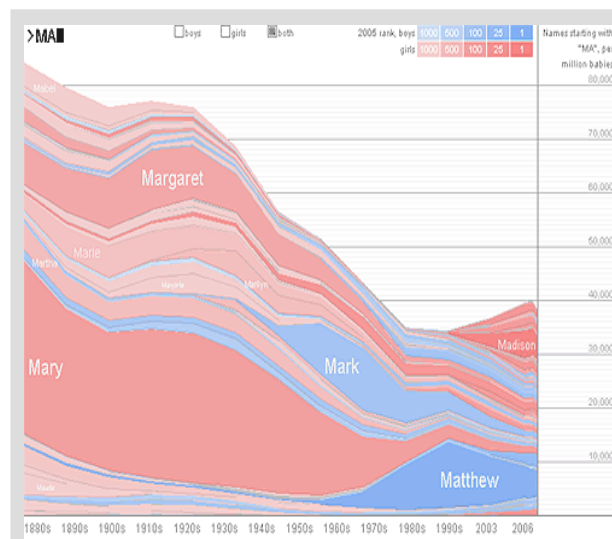
<http://kerf.cs.dartmouth.edu/backhoe/>

- 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