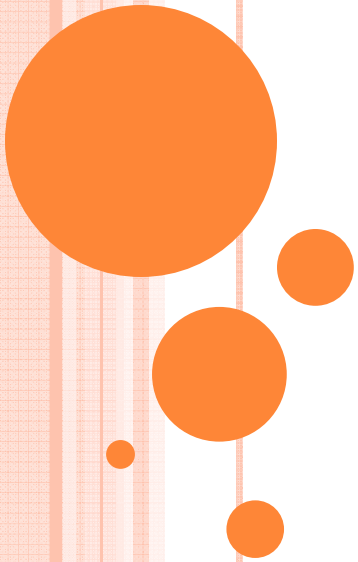


Network Flow Analysis

Blackhat USA 2008

Bruce Potter

gdead@shmoo.com

bpotter@pontetec.com

INTRODUCTIONS

- Bruce Potter
  - Founder of Ponte Technologies
    - Focus on advanced defensive technologies
  - Founder of The Shmoo Group
    - We run ShmooCon as well as other events
  - Co-author of several books and other stuff
    - *802.11 Security*
    - *Mastering FreeBSD and OpenBSD Security*
    - *Mac OS X Security*
- Don't believe anything you hear in Vegas
  - It's mostly made up for publicity, either personal or corporate
  - We're not formally trained… we shoot from the hip

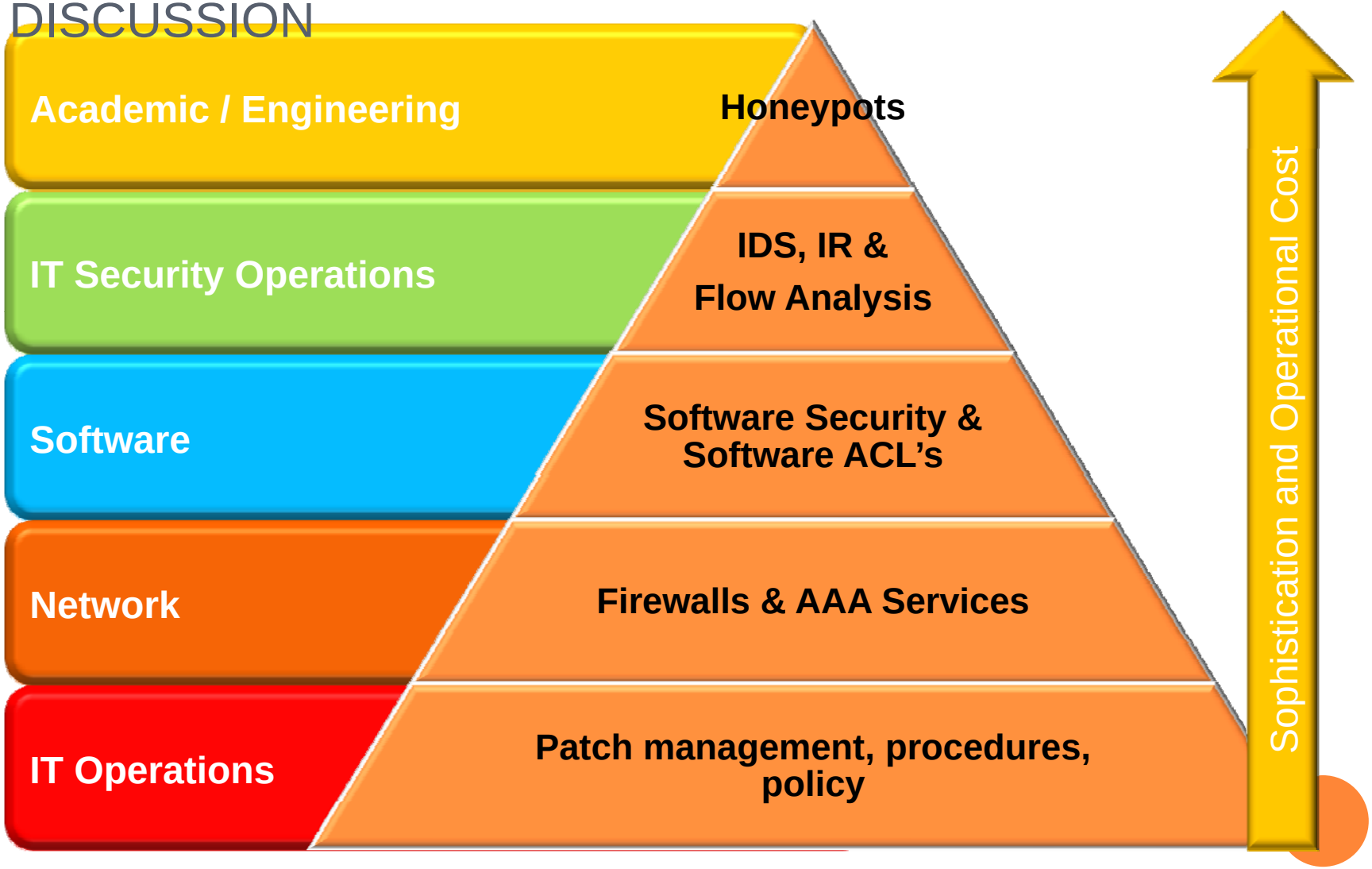
First, a Plug

- No, I don't get paid for this
- We'll be talking a lot about data representation and visualization
- This is not something to be entered into lightly… there's a lot of science and theory behind data visualization
  - Unfortunately it's hard to bring analysis and visualization concepts to the lay person in a reasonable amount of time

Edward Tufte

- Probably best know for his slagging on PPT
  - Created the Gettysburg Address as a PPT… amusing
- Published a series of books on data representation and visualization
  - *Visual Explanations*
  - *Envisioning Information*
  - *The Visual Display of Quantitative Information*
  - *Beautiful Evidence*
- Teaches 1 day classes around the country on data representation and visualization.
  - Again, I'm not paid for any of this, but I seriously recommend you go if you can
- http://www.edwardtufte.com/tufte/
  - It's darn near a religious experience for some

LET'S HAVE SOME STRUCTURE TO OUR DISCUSSION



What is Network Analysis?

- Quite simply, looking at evidence on or from the network in order to determine information regarding any of the following:
  - Security
  - Availability
  - Performance
  - Capability
  - Integrity
  - … really, any of the “ilities” (yes, performance is an “ility” ☺)

Means for Executing Network Analysis

- Basically, *analysis* involves
  - Collecting and storing data
  - Distilling and stirring the data around
  - Analyzing the results
- Lots of ways to get evidence from the network
  - SNMP data from routers and switches
  - Raw packet captures
  - Auditing information from existing network infrastructure (IDS, Firewalls, VPN gateways
  - Network Flows
- Each has various advantages and disadvantages
  - Many existing products
  - However, doing “analysis” with these products takes work… and do you really have time to do analysis or should you be configuring your firewall and fighting other fires in your network?

A View of Current Threat Space

Highly Targeted

Insider Threat

Skilled, Motivated

Org Crime, Nation State

General Purpose

Worms, virus,

Written Off

Or at least basically ignored. Very difficult with today's technology.

"Solved" Problem

AV, AS, IDS, Firewalls.

These tools are highly automated and geared towards compliance.

A View of Current Threat Space

Highly Targeted	Skilled, Motivated	General Purpose
Insider Threat	Org Crime, Nation State	Worms, virus,

Written Off	???	"Solved" Problem
Or at least basically ignored. Very difficult with today's technology.	Requires some manual work as well as a different set of tools than is currently available.	AV, AS, IDS, Firewalls. These tools are highly automated and geared towards compliance.

Need to make analysts more effective

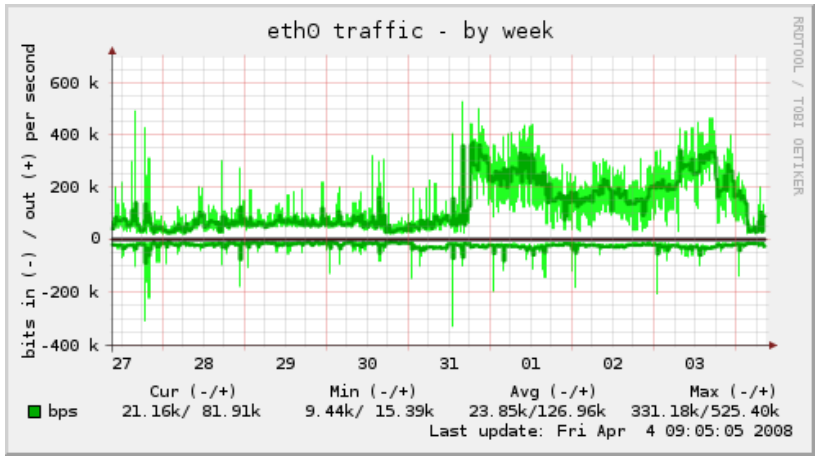
Collect, distill, and analyze the data. Not complicated, and lots of prior art. However for the public security product space,

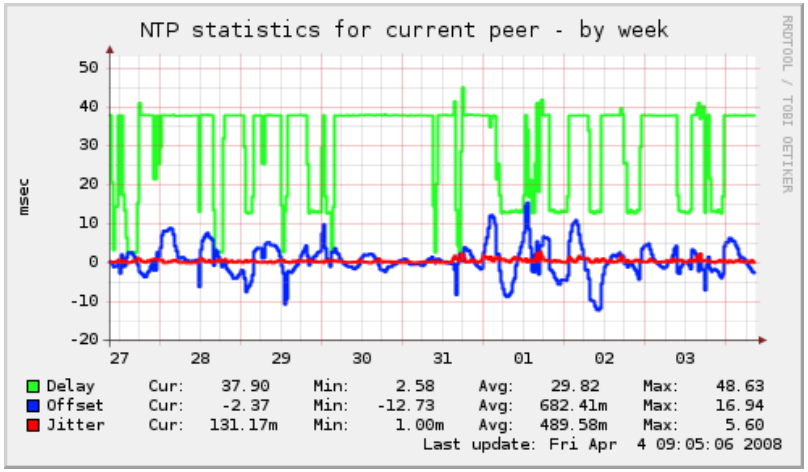
it might as well be rocket science

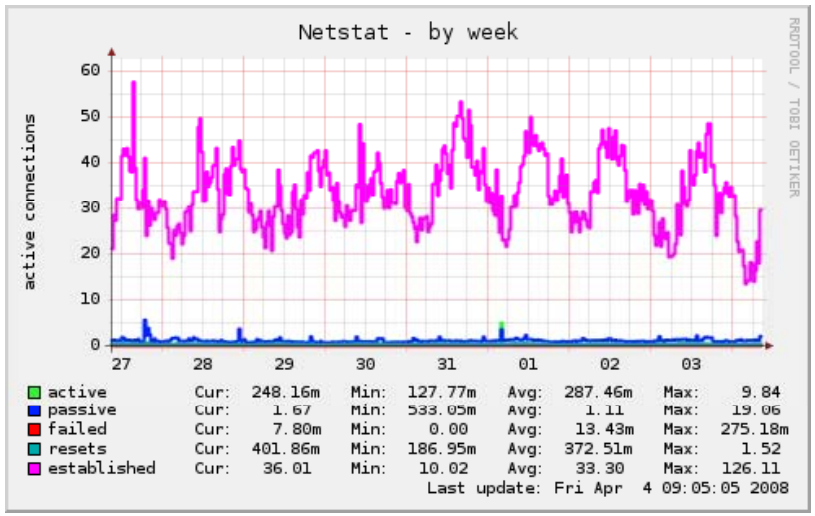
Types of Security Analysis to be Performed - Depth first vs. Breadth first

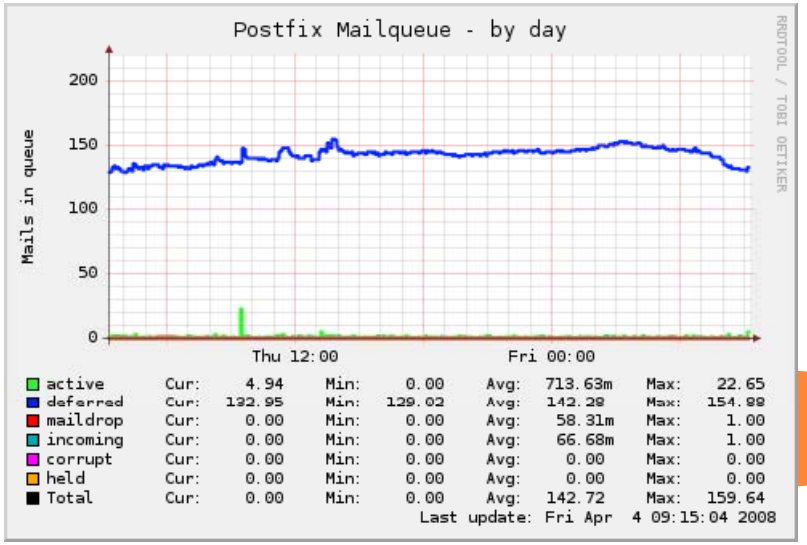
- Depth first
  - Depth first security analysis is what forensic analysts usually do
  - This type of analysis makes sense when you already know what you're looking for or where you're going to find it
  - Unfortunately it's also the type of analysis that many ad hoc security analysts end up doing
    - Tools like grep and normal shell scripting foo lead to this type of analysis
- Breadth first
  - Much more useful when you don't know what you're looking for or where to look
    - The reality for most enterprises
  - Requires more specialized tools to help distill the data first

What Do These Graphs Have in Common?









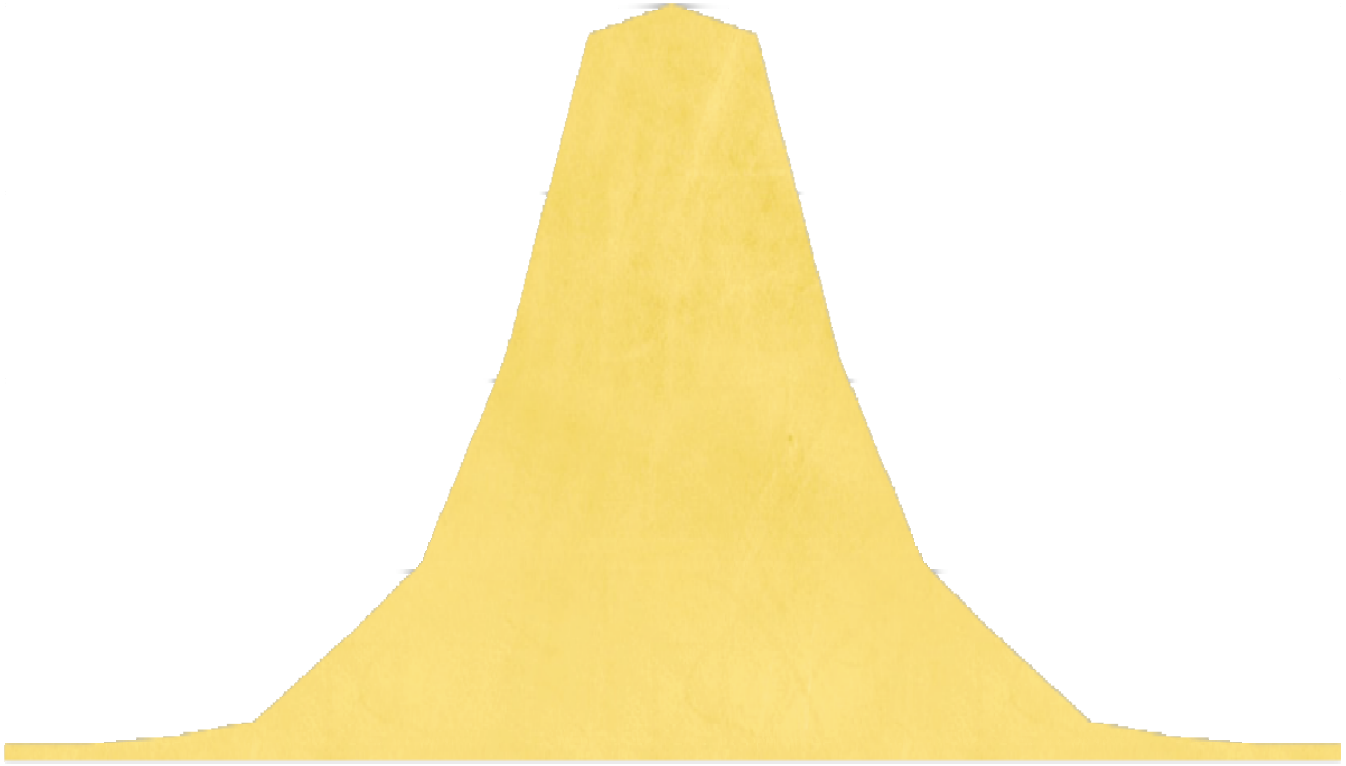
Types of Security analysis – Time Domain vs. Frequency Domain

- Time Domain analysis is common with most "enterprise management" tools.
  - Most operators care about what's going on minute to minute and how that compares what happened a minute/hour/day/week ago
  - OSS tools like MRTG have made a lot of ppl very happy over the years.
  - Unfortunately tools like MRTG have created blinders on most operators who end up believing time series analysis is THE ONLY analysis

Limitations of Time Domain Analysis

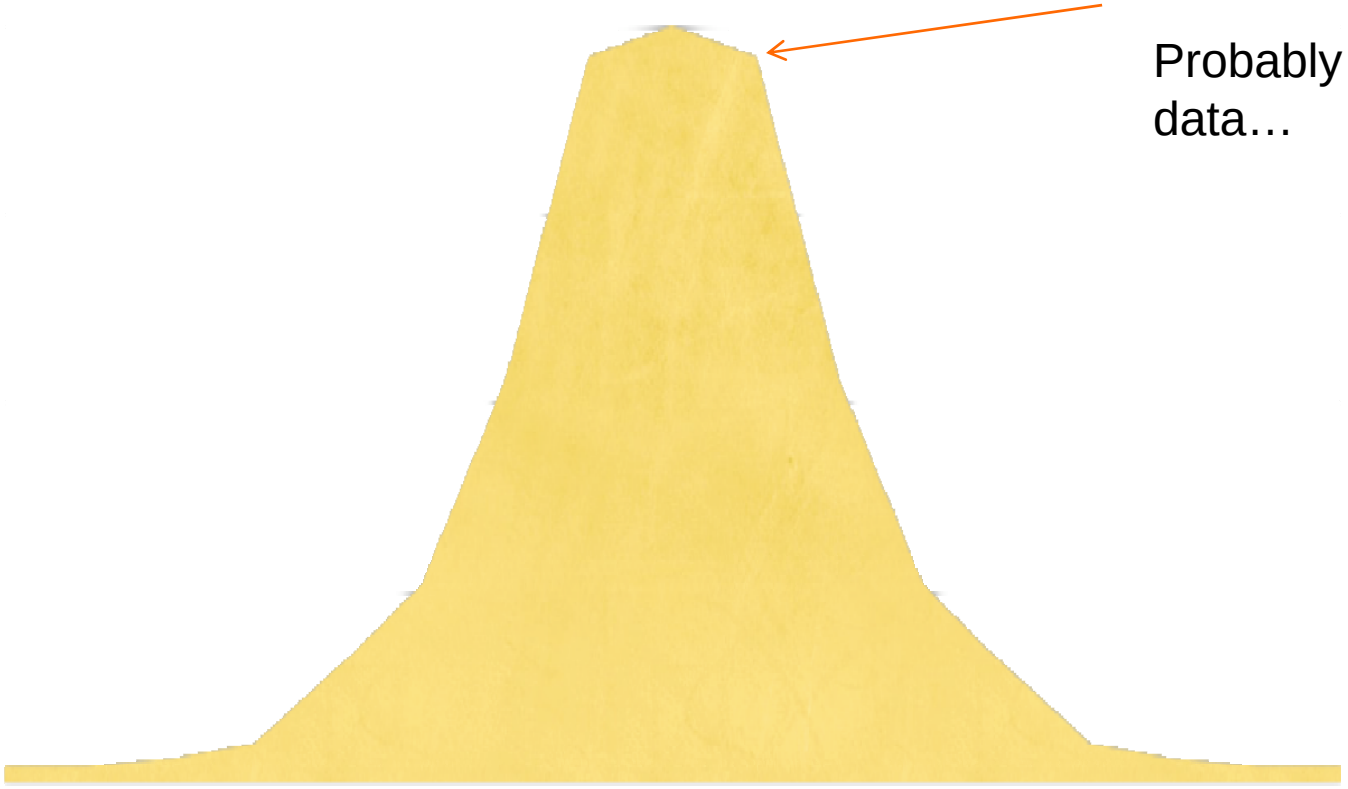
- There are others aspects of the data that get lost in the process of rolling everything together to make a pretty graph that varies over time
  - Per host, who is sending the most data outbound? Who is pulling in the most data?
  - Per host, who is talking to the most DSL hosts? The most Asia-Pacific hosts?
  - How many hosts are speaking more than 3 protocols? 4? 5? 100?
- Time domain analysis won't tell you any of these answers
  - MRTG and the other tools are NOT geared up towards this.

What is This graph?



Could be anything…. Size of emails? Traffic sent per host?
Number of hosts spoken to per host? Documents printed per day?

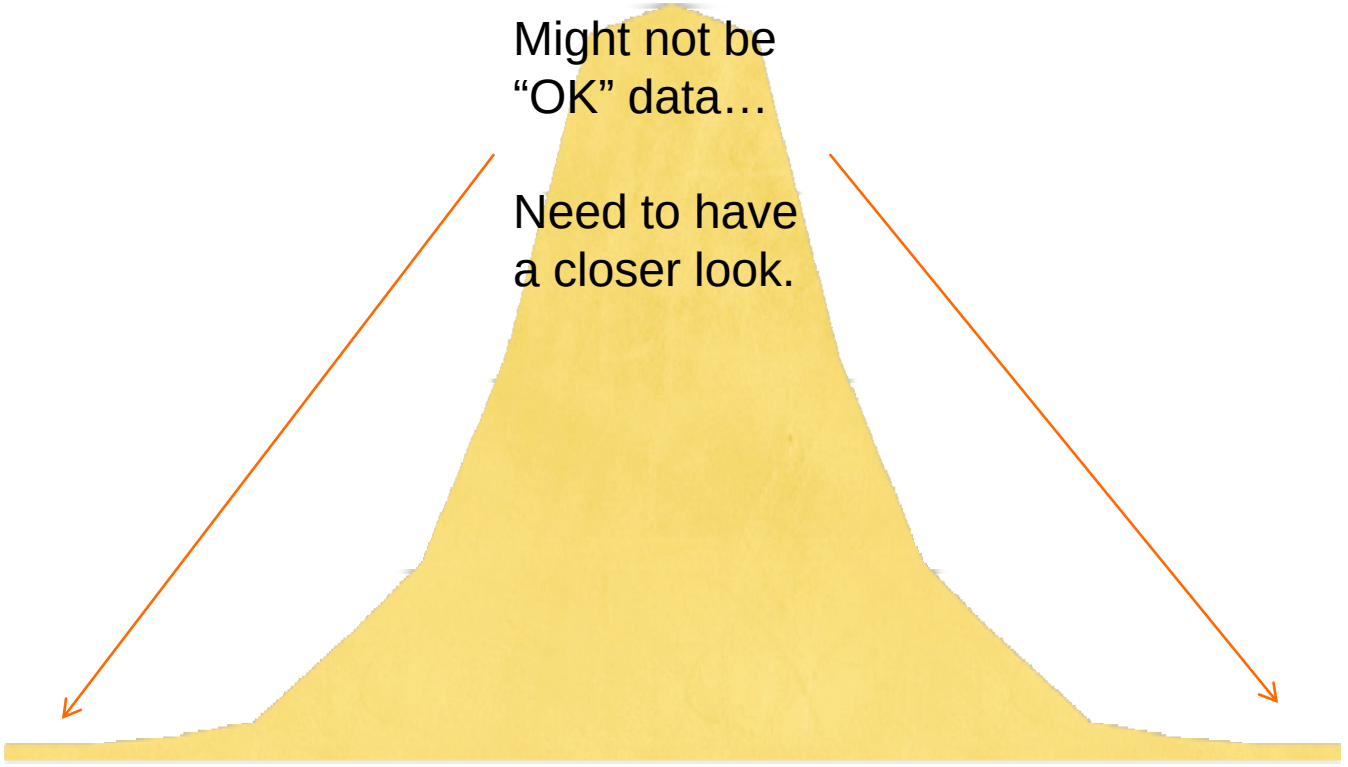
What is This graph?



Probably OK data…

Could be anything…. Size of emails? Traffic sent per host? Number of hosts spoken to per host? Documents printed per day?

What is This graph?



Could be anything…. Size of emails? Traffic sent per host?
Number of hosts spoken to per host? Documents printed per day?

What is a Flow?

- Data regarding a unidirectional flow of information through a network
  - Nothing more complicated than that

Reasons to care about Network Flows

- Great visibility into a network without a ton of processor power required on the collection and analysis hosts
  - More detail than SNMP
  - Less complicated than full packet dumps
- Relatively cheap for the routers to export
- Your network infrastructure is already inline and sees all your data
- Netflow records take up little bandwidth
- Advanced statistical analysis can undercover policy violations, bot nets, malware, etc..

Frequency Domain Analysis

- Looking at how often an event occurred per a given metric (per host, per subnet, per protocol, etc) rather than *when* an event occurred in relation to other events
  - Not a complicated concept
  - However, it is a concept geared more toward *analysts* rather than *operators*.
  - Few tools available today are focused on analyzing data; rather the tools are designed to fix a current problem and move on.

Other Types of Analysis

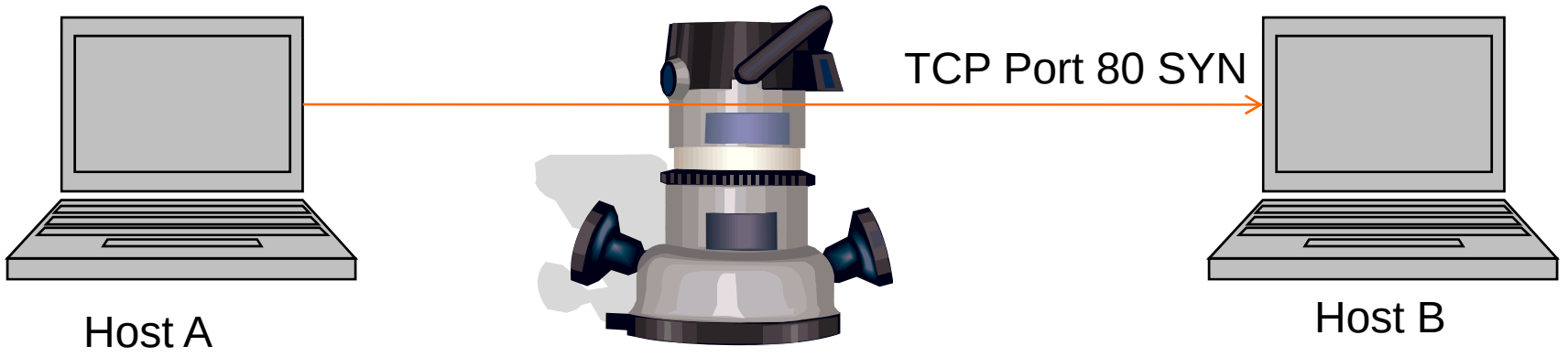
- Things can get really complicated beyond these basics
  - Correlation within a dataset – “how often was traffic with >2 ratio of outbound traffic going to Asia on weekends”
  - Correlation across multiple datasets – “How often is a small HTTP outbound connection followed by a login from the domain controller”
- These types of analysis get computationally expensive
  - But certainly not impossible. Q1Labs Qradar product does a good job of correlating data as it’s coming in. NetWitness does an *amazing* job at it, but it’s really a huge product to bring in house.

What is a Flow?

- Data regarding a unidirectional flow of information through a network
  - Nothing more complicated than that

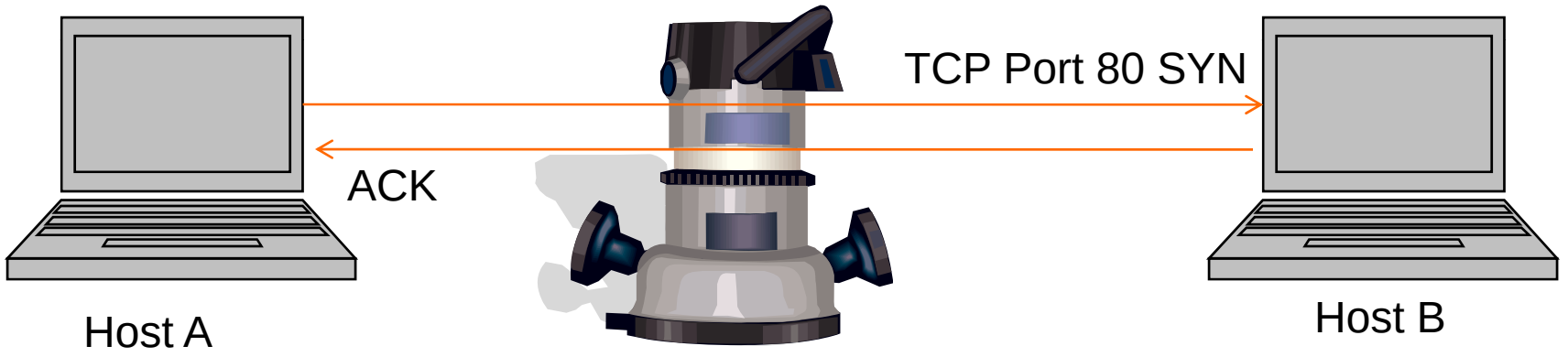
EXAMPLE

Flow1: src:A:36812, dst: B:80,



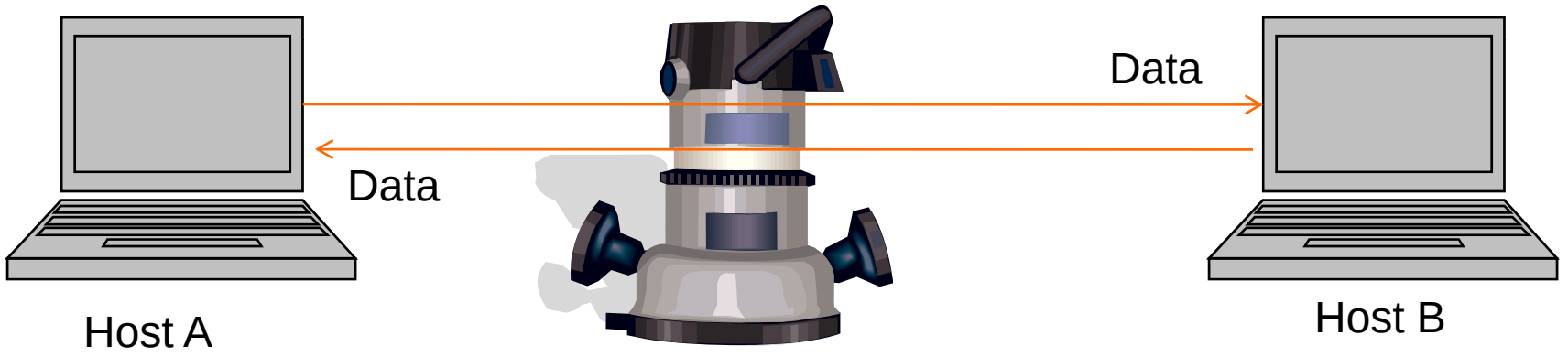
EXAMPLE

Flow1: src:A:36812, dst: B:80
Flow2: src:B:80, dst:A:36812

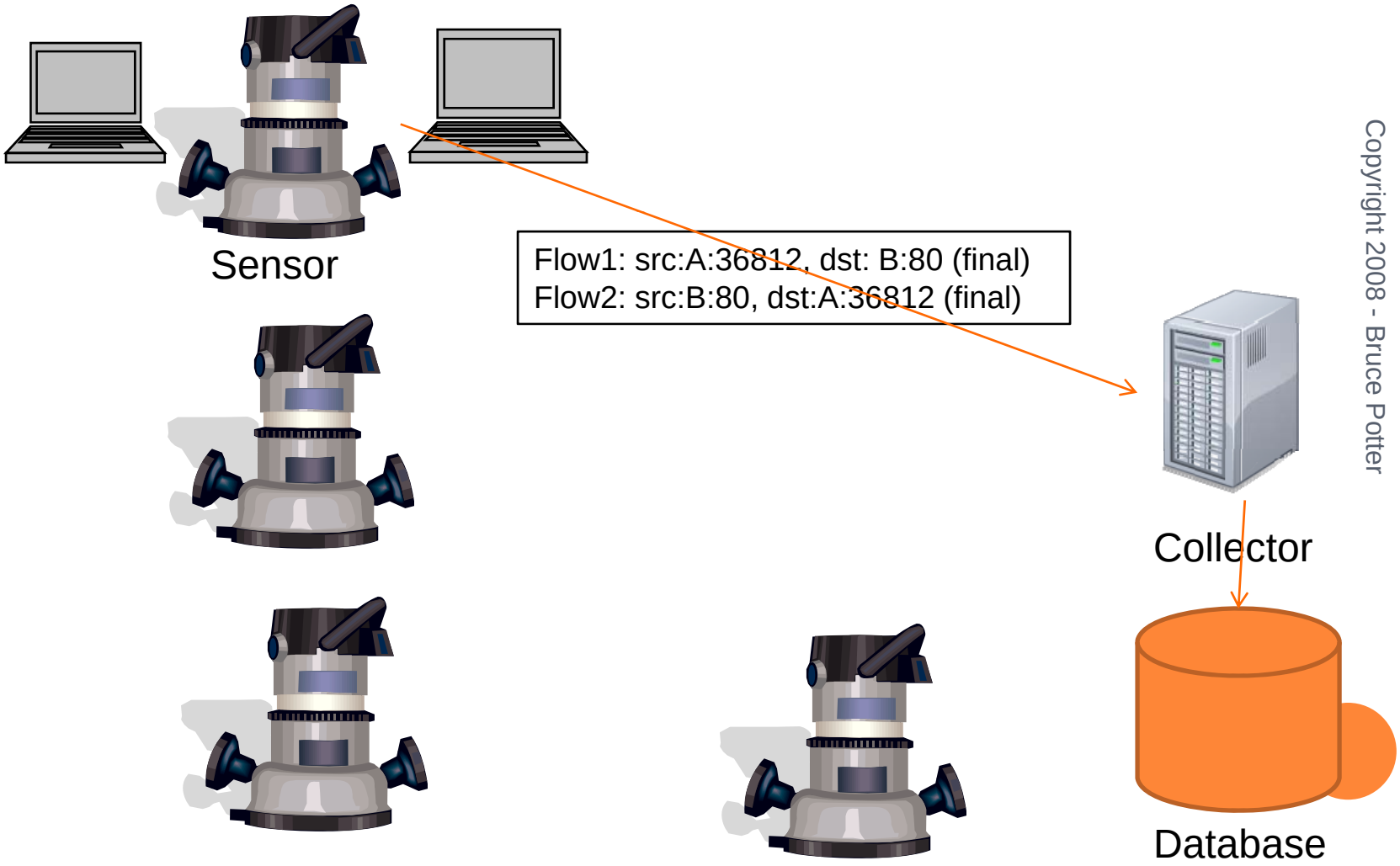


EXAMPLE

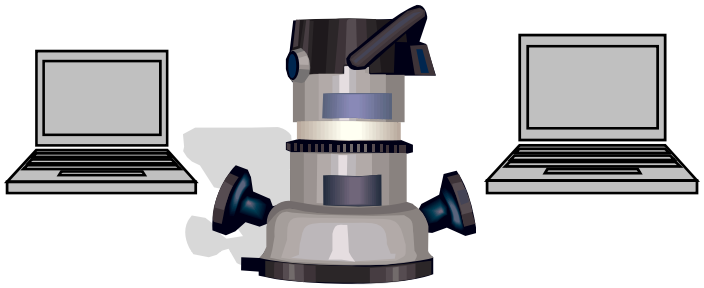
Flow1: src:A:36812, dst: B:80 (updated)
Flow2: src:B:80, dst:A:36812 (updated)



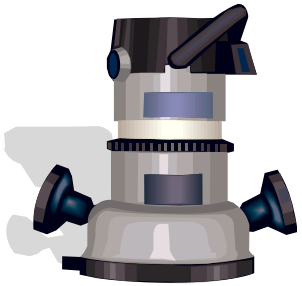
EXAMPLE

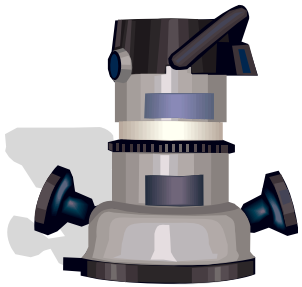


EXAMPLE

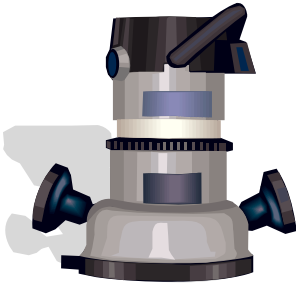


Sensor



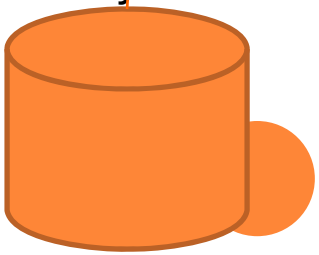


NOTE: The analysis capability may be on another host



Analyst workstation

Collector / analyzer



Database

When is a Flow Record Generated?

- Four different situations cause a flow record to be generated (general rules of thumb here, NOT set in stone!)
  - A flow terminates normally
    - Ie: a TCP session has a packet with the FIN bit set
    - Only works for session based protocols
  - The monitoring device does not see a packet in MAXIDLE time
    - Basically, if some period of time goes by (think 1-2 minutes) where no packets are seen, the router will free up memory by flushing the flow and presuming it dead
    - This is usually a tunable option. Low values may give false positives but keep the memory footprint small. High values give better data but can make for HUGE mem requirements

When is a Flow Record Generated?

- Full Cache – The router is getting pushed too hard
- The monitoring device sees active data for more than MAXACTIVE time
  - There are times when a session might run for a LONG time.
  - Rather than get one flow record for it at the very end that throws everything off, a flow will be expired.
  - This does NOT mean a router closes the session… just the accounting information gets flushed
  - Again, this is usually tunable. Think 5-30 minutes
  - It should be noted that because of these types of issues, netflow data does not make good realtime bandwidth monitoring feeds.
    - Huge FTP downloads, with a 30 min MAXACTIVE timer will show huge spikes in bandwidth use, sometimes dramatically exceeding the maximum available real bandwidth
    - Use SNMP traffic data instead… much more accurate

Doing Real Time Traffic Analysis

- If you do want to use NetFlow to monitor bandwidth, then you'll have to futz with the timers
  - Terminating flow accounting on a flow that's reached MAXACTIVE does not mean the flow is done
  - Your collector should be able to put the pieces back together
    - Either based on heuristics or on TCP flags (if it's TCP based)
  - Example – Set the active timer on your router to 1 minute
    - Certainly, this prematurely terminate the accounting record and generate multiple flows
    - Your collector may have MAXACTIVE set to 6 hours. Many few flows will be terminated incorrectly and most flows will be reconstructed by the collection engine
    - This gives you 1 minute resolution on traffic
  - Not good enough? Do port monitoring on your switches and graph that ☺

HARDWARE IMPLICATIONS

- Check the router to see what it's got left in the CPU and memory buckets

```
rtr#show proc cpu
CPU utilization for five seconds: 37%/35%; one minute: 42%; five minutes: 41%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 8180 2013277 4 0.00% 0.00% 0.00% 0 Load Meter
2 14255652 130927068 108 0.00% 0.05% 0.06% 0 OSPF Hello
3 88398944 874468 101089 0.00% 0.58% 0.68% 0 Check heaps
4 221640 408951 541 0.00% 0.00% 0.00% 0 Pool Manager
5 0 2 0 0.00% 0.00% 0.00% 0 Timers
6 32457048 72469861 447 0.00% 0.00% 0.00% 0 ARP Input
Etc...
router>show processes memory
Total: 106206400, Used: 7479116, Free: 98727284
PID TTY Allocated Freed Holding GetbufsRetbufs Process
0 0 81648 1808 6577644 0 0 *Init*
0 0 572 123196 572 0 0 *Sched*
0 0 10750692 3442000 5812 2813524 0 *Dead*
1 0 276 276 3804 0 0 Load Meter
2 0 228 0 7032 0 0 CEF Scanner
3 0 0 0 6804 0 0 Check heaps
Etc…
```


Building your Own?

- You'll need a box or two…
  - You want reliable boxes. It should be noted that these boxes will be *inline* with your network. So they should be as reliable as an ethernet cable
  - Needs to be able to handle the flow generation software without much hassle
    - Not really too hard. You can easily push wirespeed 100Mb/s on a 1GHz processor with an Linux distro.
    - Need a fair bit of memory (1GB should do fine, might get away with 512MB).
    - Disk is not an issue because the sensor won't be storing the data
  - Buy fail open (fail closed?) Ethernet cards that will turn into a cable upon crash or power failure.
    - Not cheap… like $200-$500 each

SOFTFLOWD

- There are a variety of NetFlow sensors available in the OSS world
  - I'm partial to Softflowd
    - Stable, good licence
    - Easy to configure
    - http://www.mindrot.org/projects/softflowd/
  - Runs quickly and easily on Linux and FreeBSD (w00t! Go FreeBSD!)
- The basic idea is that you create a bridge group of two ethernet interfaces
  - This is allows you to drop a softflow box inline without modifying any of your IP/subnet architecture
- Then bind softflowd to the bridge group and tell it where to export the flows
  - That's it…

Cisco Router

```
# Assume that fe 0/1 is the inbound from
  the Interenet and fe0/2 is the LAN facing
  interface
router(config)#interface FastEthernet 0/1
router(config-if)#ip route-cache flow
router(config-if)#exit
#since by default this is only for inbound,
  repeat for the other interface
router(config)#interface FastEthernet 0/2
router(config-if)#ip route-cache flow
router(config-if)#exit
```


Cisco Router

```
#configure the netflow collector IP and port
router(config)#ip flow-export destination
  192.168.90.10 9996
#by default, the flows will be sourced from
  lo0.. change if needed
router(config)#ip flow-export source
  FastEthernet 0/1
router(config)#ip flow-export version 5
#super aggressive timeout for active to keep
  data flowing into the collector (mins)
router(config)#ip flow-cache timeout active 1
#also aggressive (seconds)
router(config)#ip flow-cache timeout inactive 15
```

CHECKING UP

```
show ip cache flow
   IP packet size distribution (489639251 total packets):
      1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
      .000 .992 .000 .003 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .000 .000 .000 .000 .003 .000 .000 .000 .000 .000 .000
```


CHECKING UP

```
IP Flow Switching Cache, 8913408 bytes
     5088 active, 125984 inactive, 1843766371 added
     805412120 ager polls, 0 flow alloc failures
     Active flows timeout in 30 minutes
     Inactive flows timeout in 15 seconds
     last clearing of statistics never
   Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
   Idle(Sec)
   --------           Flows     /Sec     /Flow  /Pkt     /Sec      /Flow      /Flow
   TCP-Telnet         28084      0.0         1    45      0.0       0.1       11.7
   TCP-FTP           172835      0.0         1    47      0.0       2.4       13.7
   TCP-FTPD            2818      0.0         1    40      0.0       0.2       11.3
   TCP-WWW          5551226      1.2         1    53      1.3       0.1        5.0
   TCP-SMTP            4179      0.0         1    42      0.0       1.0       12.2
   TCP-X               2594      0.0         1    40      0.0       0.6       11.2
   TCP-BGP             2546      0.0         1    40      0.0       0.2       11.5
   TCP-NNTP            2554      0.0         1    40      0.0       0.1       11.2
   TCP-Frag             177      0.0         2   269      0.0       1.7       16.8
   TCP-other         528636      0.1         1    40     65.5       0.6       35.5
   UDP-DNS            11596      0.0         1    54      0.0       0.8       17.2
   UDP-NTP              723      0.0         2    40      0.0       9.0       16.8
   UDP-TFTP             763      0.0         3    37      0.0      10.2       16.9
   UDP-Frag              25      0.0         1    40      0.0     251.4       15.0
   UDP-other      169720402     39.5         1    40     46.2       0.6       11.3
   ICMP              275131      0.0        10   759      0.6       7.7       14.2
   IGMP                  36      0.0      1789  1246      0.0      15.2       16.9
   IP-other               7      0.0        19    64      0.0      18.9       17.5
   Total:         176304332     41.0         2    44    113.9       0.6       11.2
```

CHECKING UP

```
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcPDstP  Pkts
   Hs9/1/0        192.168.2.51    Null           1.1.1.1         11 04A9 0017   614K
   Hs9/1/0        192.168.47.72   Null           1.1.1.1         11 05F9 0017   281K
   Hs9/1/0        192.168.49.52   Null           1.1.1.1         11 08EA 0017    65K
   Hs9/1/0        192.168.32.18   Null           1.1.1.1         11 08EC 0017  1463K
   Hs9/1/0        192.168.208.208 Null           1.1.1.1         11 0411 0017  8351K
   Hs9/1/0        192.168.77.66   Null           1.1.1.1         11 126F 0017  1763K
   Hs9/1/0        192.168.184.159 Null           1.1.1.1         11 0609 0017   191K
   Hs9/1/0        192.168.22.48   Null           1.1.1.1         11 0885 0017  1520K
   Hs9/1/0        192.168.22.48   Null           1.1.1.1         11 0883 0017    66K
   Hs9/1/0        192.168.7.44    Null           1.1.1.1         11 0F07 0017    97K
   Hs9/1/0        192.168.7.44    Null           1.1.1.1         11 0F09 0017  2084K
   Hs9/1/0        192.168.54.208  Null           1.1.1.1         11 040C 0017  3018K
   Hs9/1/0        192.168.248.90  Null           1.1.1.1         11 0521 0017   201K
   Hs9/1/0        192.168.201.177 Null           1.1.1.1         11 060C 0017   171K
   Hs9/1/0        192.168.201.177 Null           1.1.1.1         11 054C 0017   107K

etc. . .
```


What Exactly Are You Looking For?

- As much fun as it is to just dig through the data, you tend to have a purpose for looking through it
  - The purpose of your analysis will drive the mans of your analysis
- Bots / malware
- Data exfiltration
- Policy violations
- Performance / utilization

Finding Bots

- Look for traffic on standard bot/malware ports
  - TCP/UDP 53
  - 6666, 6667 (IRC)
- Hard to find port 80 bots, but not impossible
  - Look for large # of connections with little bandwidth used
- Examine destination address… might want to look for data going to places you don't trust
  - http://www.apnic.net/db/min-alloc.html

Data Exfiltration

- Heavy outbound vs inbound data
  - 2:1 is a pretty good ratio to weed out the noise
  - In many non-academic environments, that's sufficient…
- May need to rule out mail hosts and VPN gateways
    - They tend to be big outbound talkers
- Ex: 2000 hosts, might see 20 flows *a day* that hit this ratio

Policy Violations

- Known bad patterns
  - Hard to track P2P/VOIP traffic – Best to look for lots of src ports talking to lots of dst ports
- Have to get a good “eye” for what’s in your policy and how it manifests itself in your traffic
- Top talkers
  - GB of data a day, ever day starts to seem fishy
- Where are your sensors?
  - If it’s just on the WAN links, you’ll miss internal violations… be sure you know where your data is coming from

Performance / Utilization

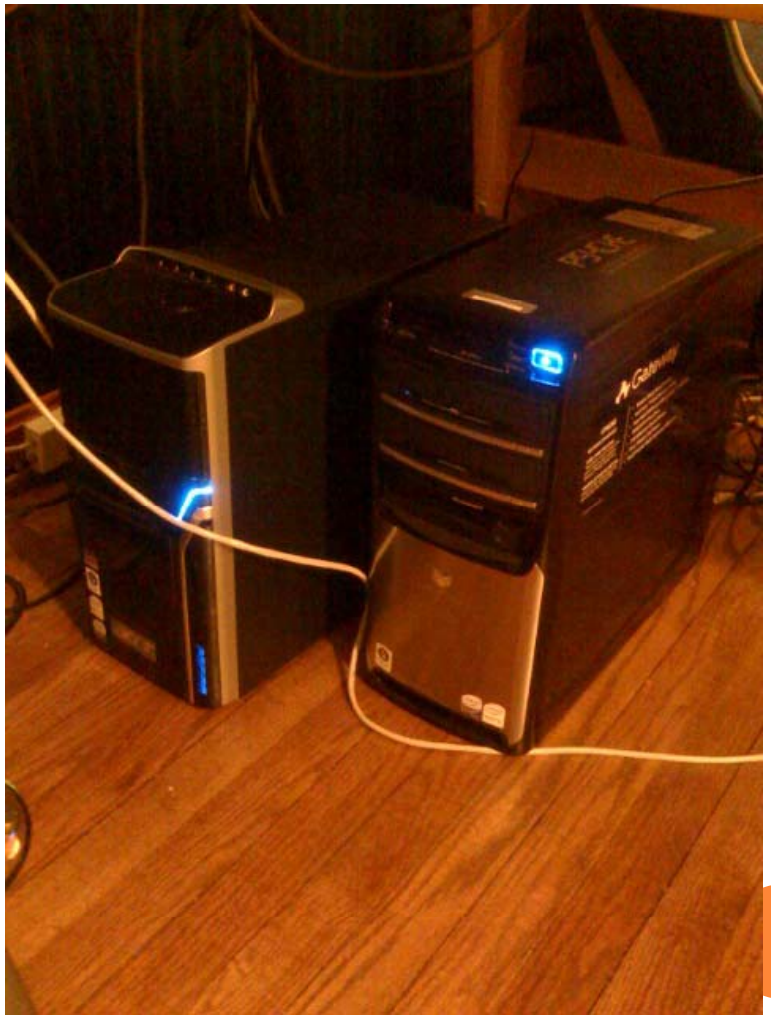
- Check out low speed links and inter-router connections
  - Obviously, look for pipes near capacity
  - Get an understanding of the types of data on the links and monitor the different types over time
- Top talkers
  - Figure out who and why
- High packet count / low packet sizes can indicate latency sensitive protocols
  - Talk to users about their experiences

Building a Collection and Analysis Host

- Analysis of flows can be very intensive
  - Data tends to get stirred on the way in, and that takes CPU and disk
  - The queries by the user can get pretty whacky, and that takes CPU, disk, AND memory
- As a point of reference, a 2000 host organization will generate about 10M flows in a day.
  - That's about 5k flows per host/day. A decent rule of thumb
  - ShmooCon had about 2M flows in a day and a half on about 150 machines

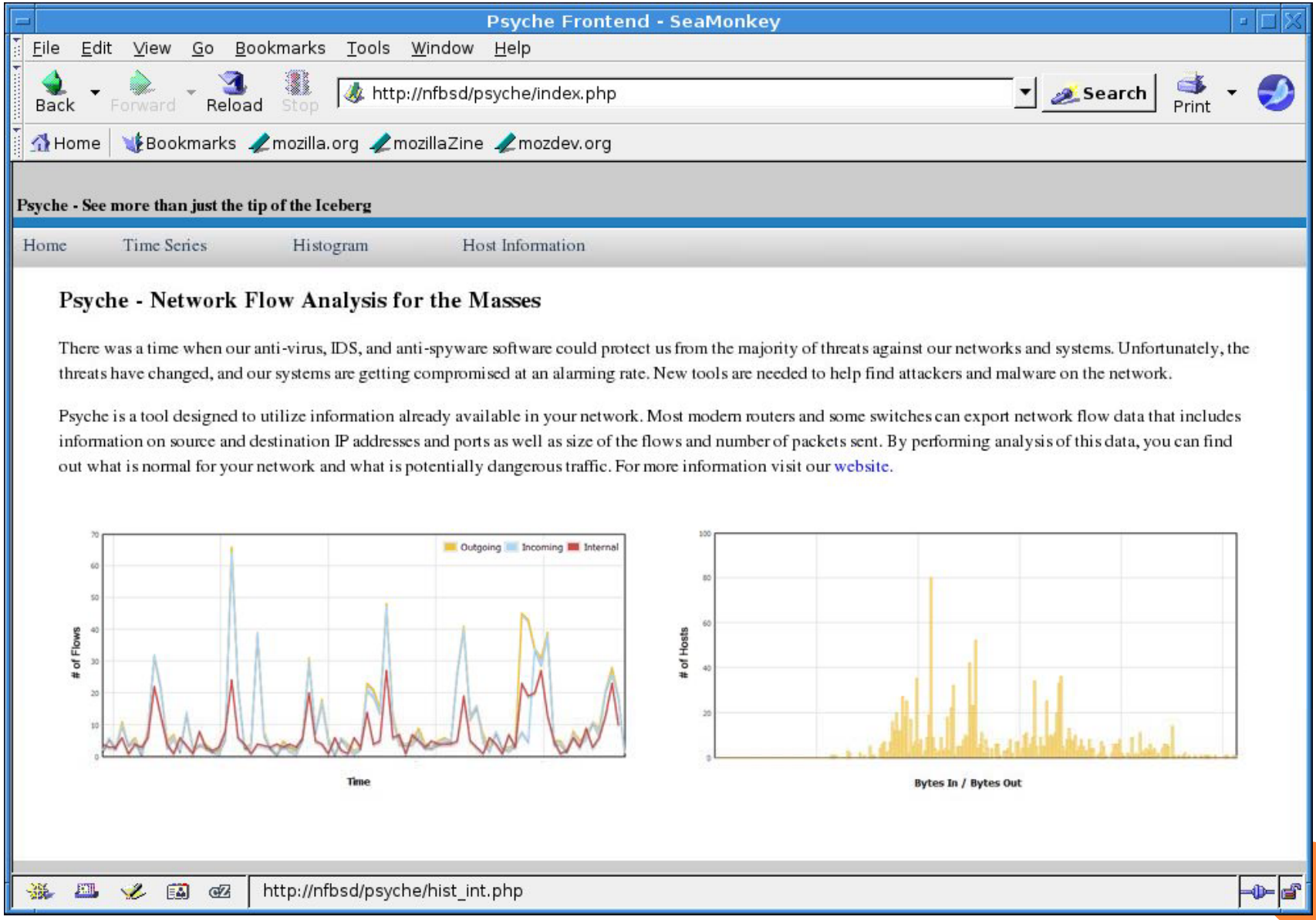
Scoping a collection machine

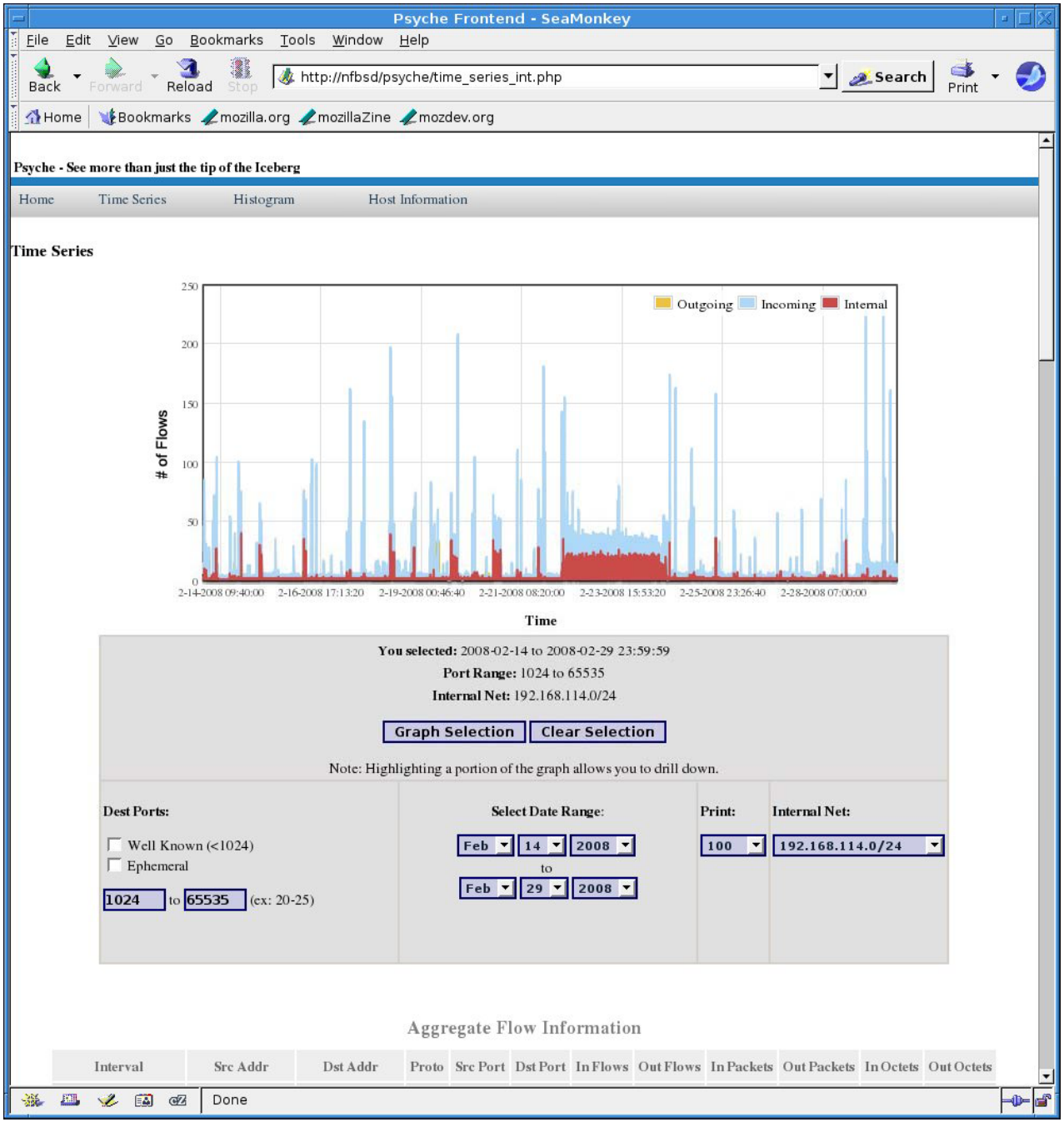
- You can do it on the sorta cheap if you want
  - Box 1 - Quad core, 3GB RAM, 500GB disk. $750
  - Box 2 - Quad core, 2 GB RAM, 400GB disk. $550
  - Extras - 3GB RAM($60), 2x500GB disk for RAID0 ($240)
  - $1500 == 2 super computers under my desk

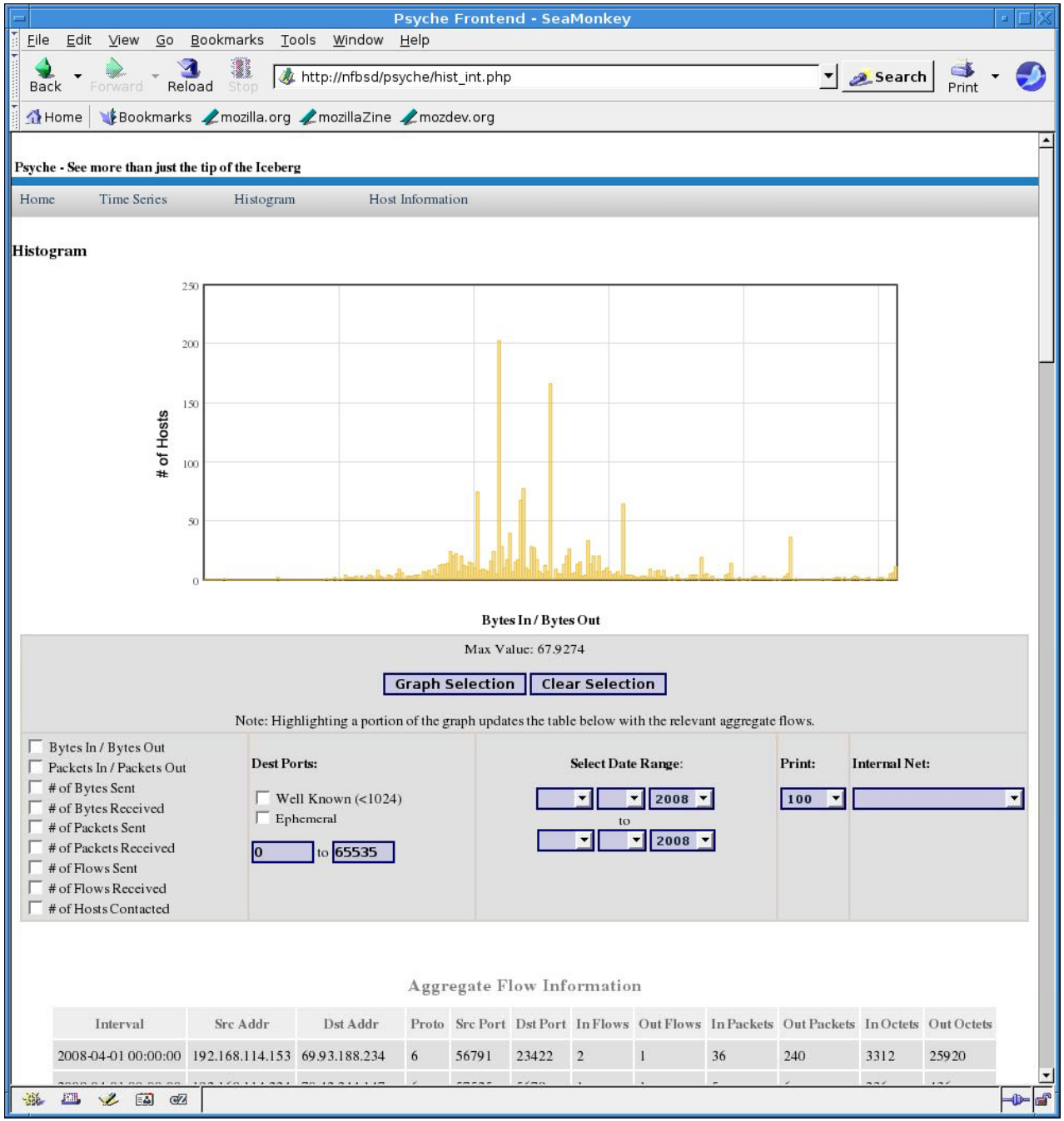


Installing Psyche

- Pretty easy. Download from http://psyche.pontetec.com/ and follow the directions
- DB == postgres. It's different than MySQL, but doesn't have the strange license issues.
- Primary testing is done against softflowd, but should work with any sensor







Parting Thoughts

- We're really just scratching the surface here
  - There are more tools, more views, more data to look at
  - For more tools, take a look at http://www.networkuptime.com/tools/netflow/
  - Really, all of these tools have the most relevance on your own network
    - You won't believe the number of "ah-ha" moments you'll have using NetFlow tools
  - You really don't need a huge box to use the RRD-based tools
    - Take a spare system off the rack and fire up NFSen. Shouldn't take more than an afternoon to configure

Contact Info

Bruce Potter

bpotter@pontetec.com