Spectral Techniques for Internet Traffic

Christos Papadopoulos and John Heidemann

USC/ISI

Data Catalog Workshop

CAIDA, June 3, 2004

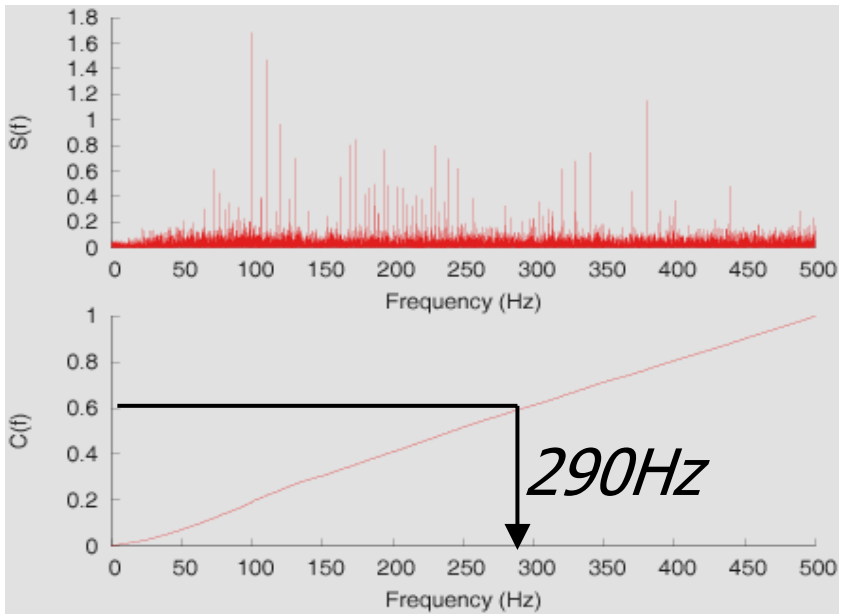
christos@isi.edu, johnh@isi.edu

Research Topics

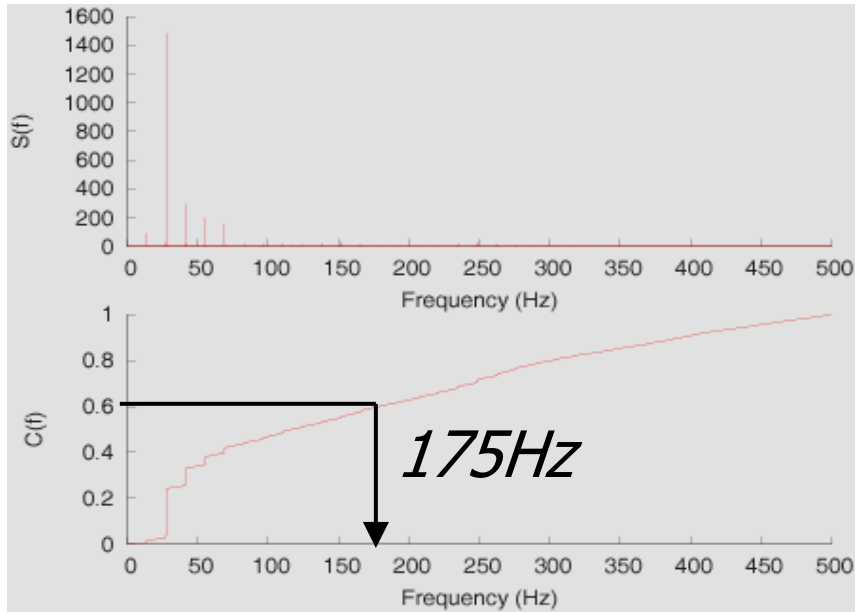
- Security
  - DDoS classification
  - Attack signatures
- Network management
  - Detection of saturated links
  - TCP dynamics
- Methodology: Spectral analysis

Single vs. Multi-source Attacks

Single-source



Multi-source



- Single src attack produces linear cumulative spectrum
- Multi-src attacks produce localization of power in low frequencies

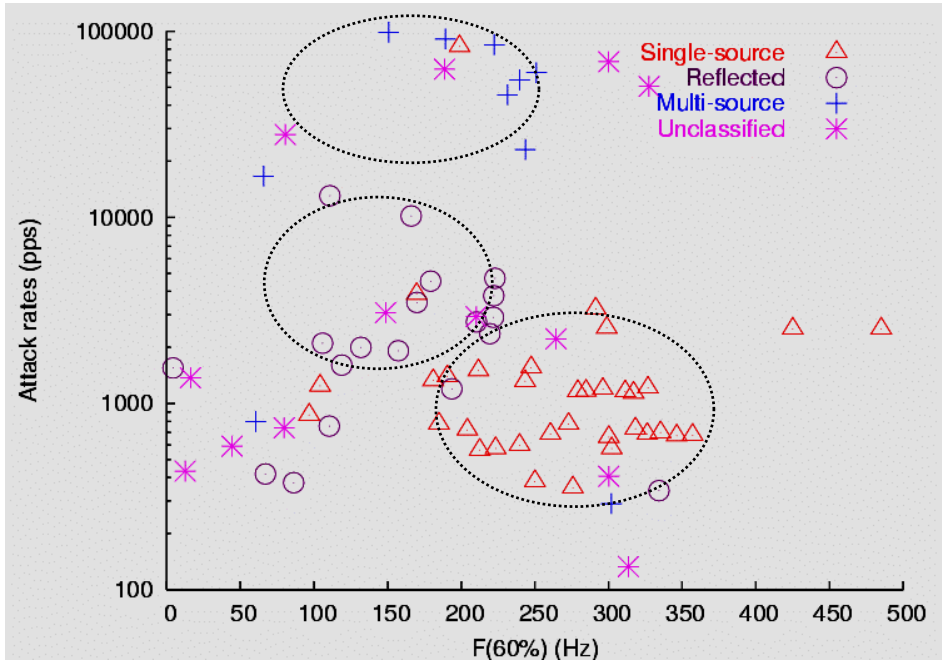
Single vs. Multi-source Attacks (cont.)

Steps:

- Compare F(60%) to identify single-/multi-source attacks
- Single-source:

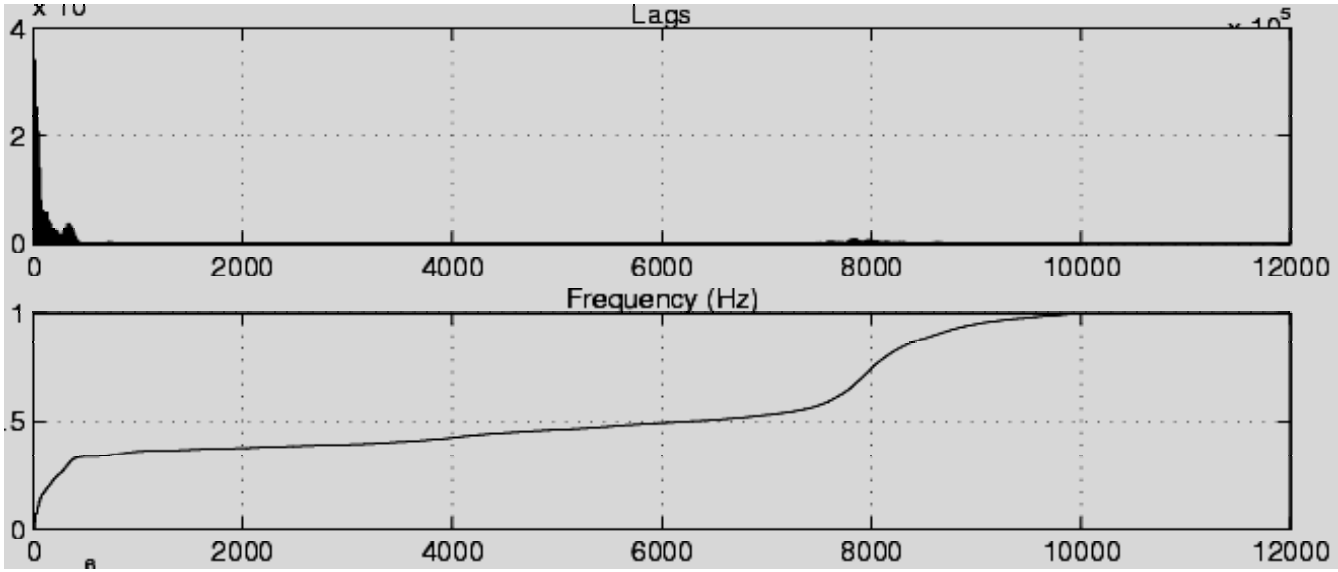
  F(60%) mean 268Hz (240-295Hz)
- Multi-source:

  F(60%) mean 172Hz (142-210Hz)
- Robustly categorize Unclassified attacks

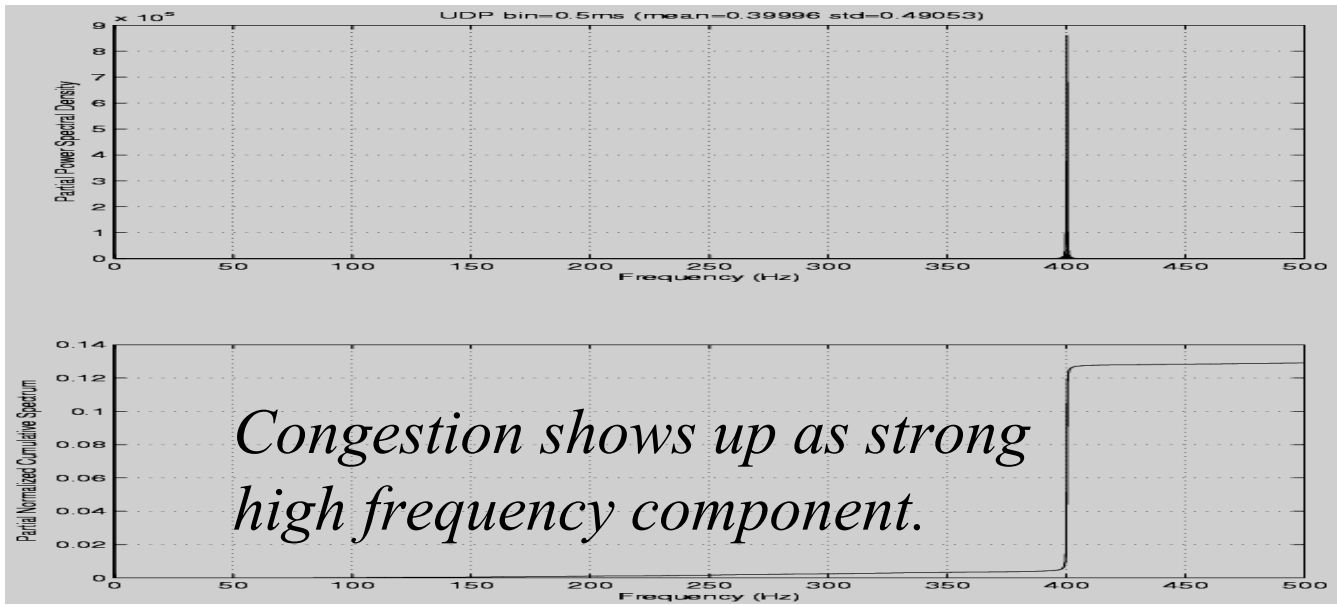


Results reported at SIGCOMM 2003, Hussain et al.

Congested vs. Un-congested Link



Un-congested Link (TCP, UMD->USC, 64MB window)

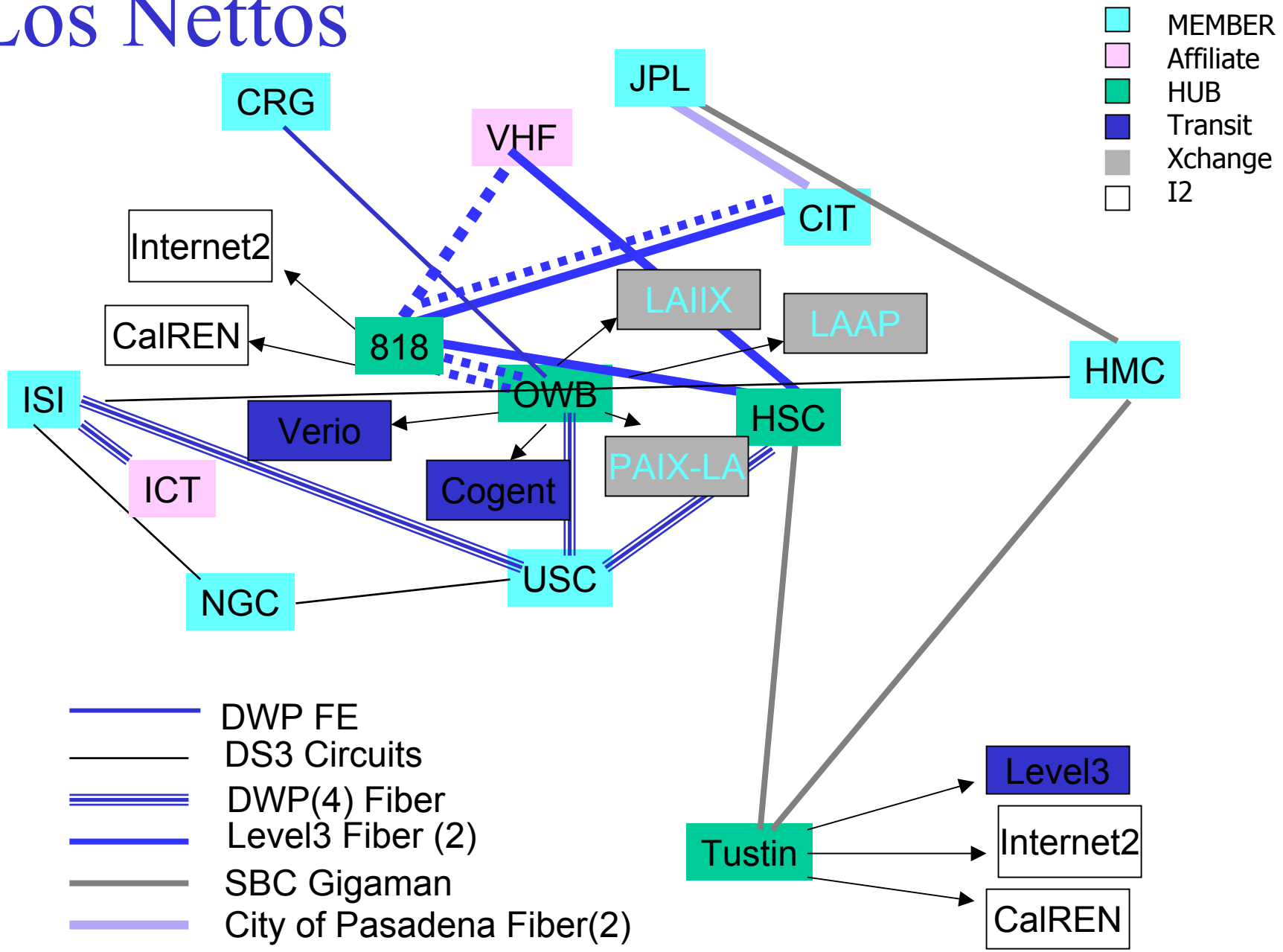


Spectrum of congested link shows clear signature.

Playground: Los Nettos

- Regional network for LA area
- ~15 years in existence
- Three upstream providers (Verio, Level3, Cogent) plus Internet 2
- 6 members and O(100) associates
  - mix of academic and commercial
- About 45K machines

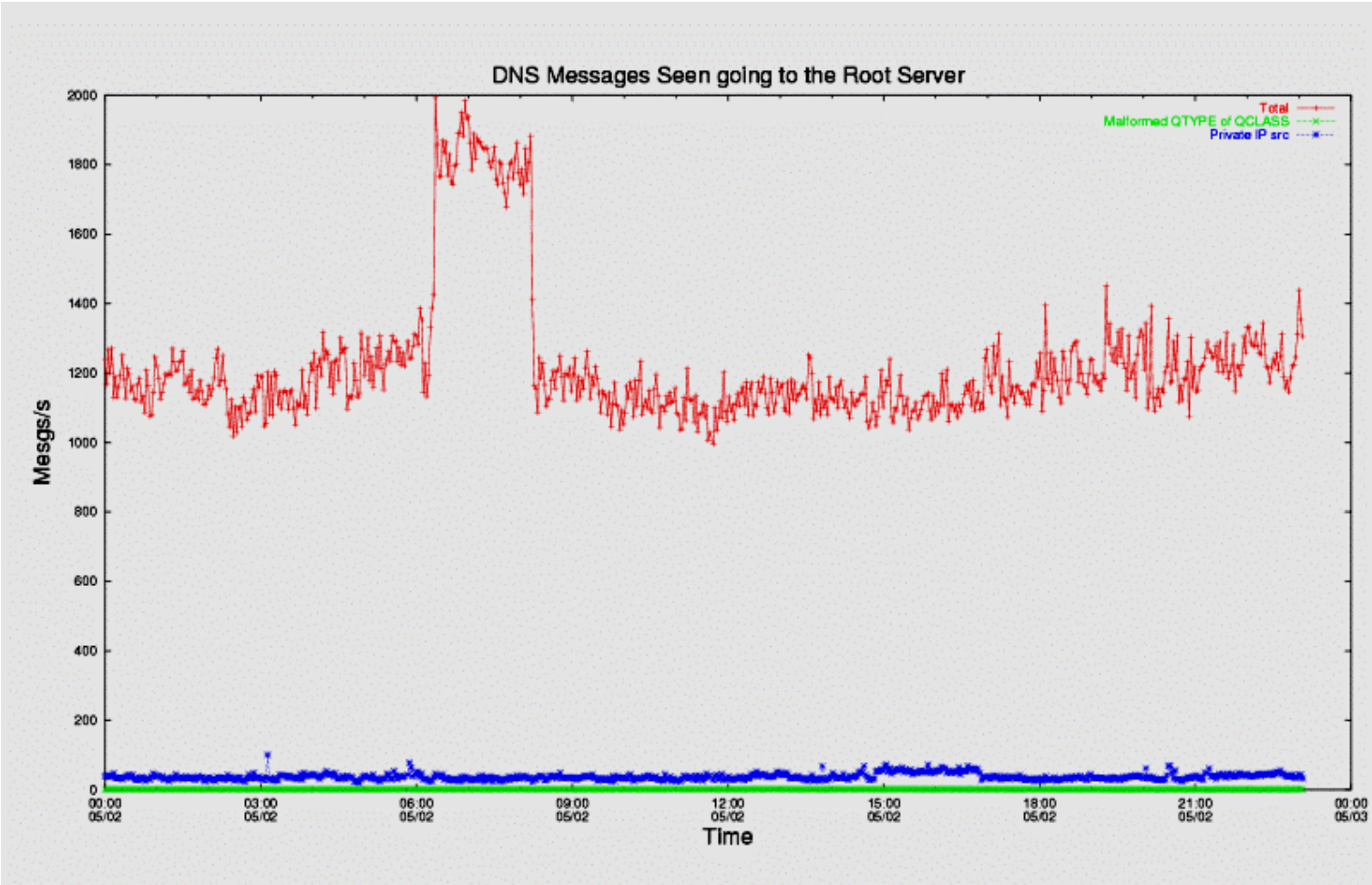
Los Nettos


MEMBER
Affiliate
HUB
Transit
Xchange
I2
CRG
JPL
VHF
CIT
Internet2
LAIIX
LAAP
CalREN
818
HMC
ISI
OWB
HSC
Verio
PAIX-LA
ICT
Cogent
USC
NGC
DWP FE
DS3 Circuits
DWP(4) Fiber
Level3 Fiber (2)
SBC Gigaman
City of Pasadena Fiber(2)
Level3
Tustin
Internet2
CalREN

Current Data Collection: Links

- Currently monitored links
  - Verio (200mbps)
  - Part of Internet 2 (in/out of USC)
- Other available links
  - Level3 (300mbps)
  - Rest of Internet 2 (200mbps)
  - Cogent (60mbps)

DNS: B and L Root Servers



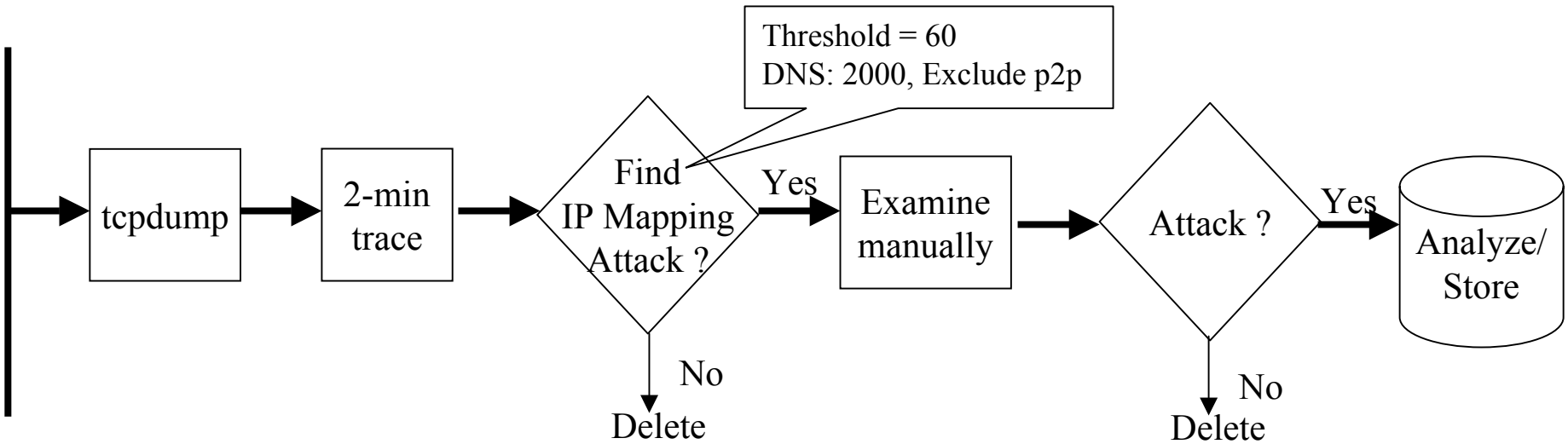
Current Data Collection: Trace Hardware

- Trace hardware
  - PCs with 250GB local disks
  - Netgear GA620 fiber cards
  - Driver tuned to partial packet capture
- RAID boxes
  - About 6TB

Current Data Collection: Trace Software

- PCs running FreeBSD
- Tcpdump
  - Headers only
- Traces saved in 2 min files on local disk
- Local analysis and periodic transfer to RAID boxes

Trace Analysis



- Captured 80 attacks (July-Nov 2002)
- Work by Alefiya Hussain

Available Traces

- All 80 DDoS attacks
  - anonymized
  - binned (1ms) time-series
- Available as a DVD
- Must sign 1-page, reasonable MOU
  - Then we mail you the DVD
- Some attacks distributed to about 8-10 takers without advertising

Our Requirements

- Packet-level traces
- Accurate, high resolution timestamps
- Metadata to describe attacks
- ..more..
- Contact {johnh@isi.edu or christos}@isi.edu for more information