Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

ADVANCED THREAT DETECTION AND FORENSICS VIA NETFLOW/IPFIX

Charles Herring
@charlesherring
cherring@lancope.com
http://f15h.co

FLOW CONCEPTS

Network Logging Basics

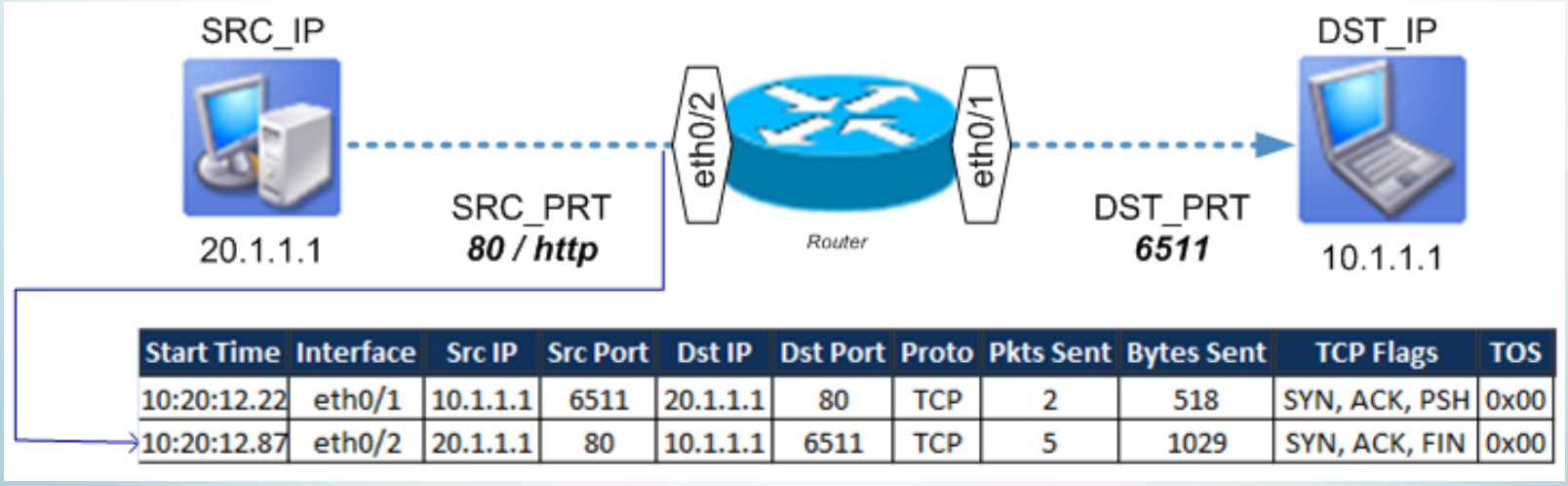
Lancope.
VISION TO SECURE,
INTELLIGENCE TO PROTECT

- A record; not a sample
- Can only log available data
- Unidirectional in nature
- Interface specific
- “Phone record” not “Phone tap”
- Category called “NetFlow” or “Flow”
- Devices with one or more Flow producing interfaces are “Exporters”
- Exporters cache and forward records to “Collectors”
- Bandwidth of “basic” Flow export is ~0.1% of monitored traffic

Logging Standards

- NetFlow v9 (RFC-3950)
- IPFIX (RFC-5101)
- Rebranded NetFlow
  - Jflow – Juniper
  - Cflowd – Juniper/Alcatel-Lucent
  - NetStream – 3Com/Huawei
  - Rflow – Ericsson
  - AppFlow - Citrix

Basic/Common Fields



Start Time	Interface	Src IP	Src Port	Dst IP	Dst Port	Proto	Pkts Sent	Bytes Sent	TCP Flags	TOS
10:20:12.22	eth0/1	10.1.1.1	6511	20.1.1.1	80	TCP	2	518	SYN, ACK, PSH	0x00
10:20:12.87	eth0/2	20.1.1.1	80	10.1.1.1	6511	TCP	5	1029	SYN, ACK, FIN	0x00

Extensible Data Fields

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Data sources can provide additional log information

Examples of Extensible Fields

- Network Based Application Recognition
- Performance Metrics (SRT/RRT, Collisions)
- HTTP Headers
- NAT Data
- Security Action (Permit/Deny)
- TTL
- DSCP
- Payload

Packet Capture of IPFIX

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

```
Cisco NetFlow/IPFIX
  Version: 10
  Length: 1412
⊞ Timestamp: Nov  6, 2012 08:15:23.000000000 Central Standard Time
  FlowSequence: 1310926
  Observation Domain Id: 22086
⊟ Set 1
    FlowSet Id: (Data) (335)
    FlowSet Length: 608
  ⊟ Flow 1
    ⊞ [Duration: 0.000000000 seconds]
      System Init Time: Oct 30, 2012 23:52:35.523000000 Central Daylight Time
      SrcAddr: 74.207.227.45 (74.207.227.45)
      DstAddr: 216.83.162.167 (216.83.162.167)
      SrcPort: 42101
      DstPort: 443
      Source Mac Address: Cisco_00:00:10 (00:08:a4:00:00:10)
      Post Destination Mac Address: Cisco_00:00:06 (00:18:ba:00:00:06)
      Octets: 44
      Packets: 1
      InputInt: 1059
      OutputInt: 1079
      Protocol: 6
      TCP Flags: 0x02
      Vlan Id: 0
      MPLS-Label1: 0 exp-bits: 0
      MinTTL: 49
      IP ToS: 0x00
      Enterprise Private entry: (LANcope, Inc.) Type 29794: Value (hex bytes): 00
      Total TCP syn: 1
      Total TCP ack: 0
      Total TCP fin: 0
      Total TCP rst: 0
```

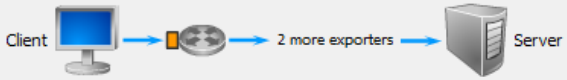
Stitching & De-duplication

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Quick View for Flow

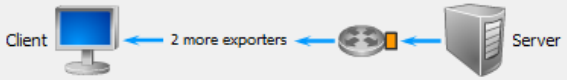
General | **Interfaces** | Table

Client Exporters IP (IF)



Exporter	Exporter...	Interface	Direction	TTL	DSCP	Flow Act...
10.240.200.2	Exporter	ifIndex-1	Outbound			
10.240.200.2	Exporter	ifIndex-2	Inbound		best_effort	
10.240.200.1	Cisco ASA	Wan	Outbound			Permitted
10.240.200.1	Cisco ASA	Lan	Inbound			Permitted
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan1	Inbound		best_effort	
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan240	Outbound			

Server Exporters IP (IF)

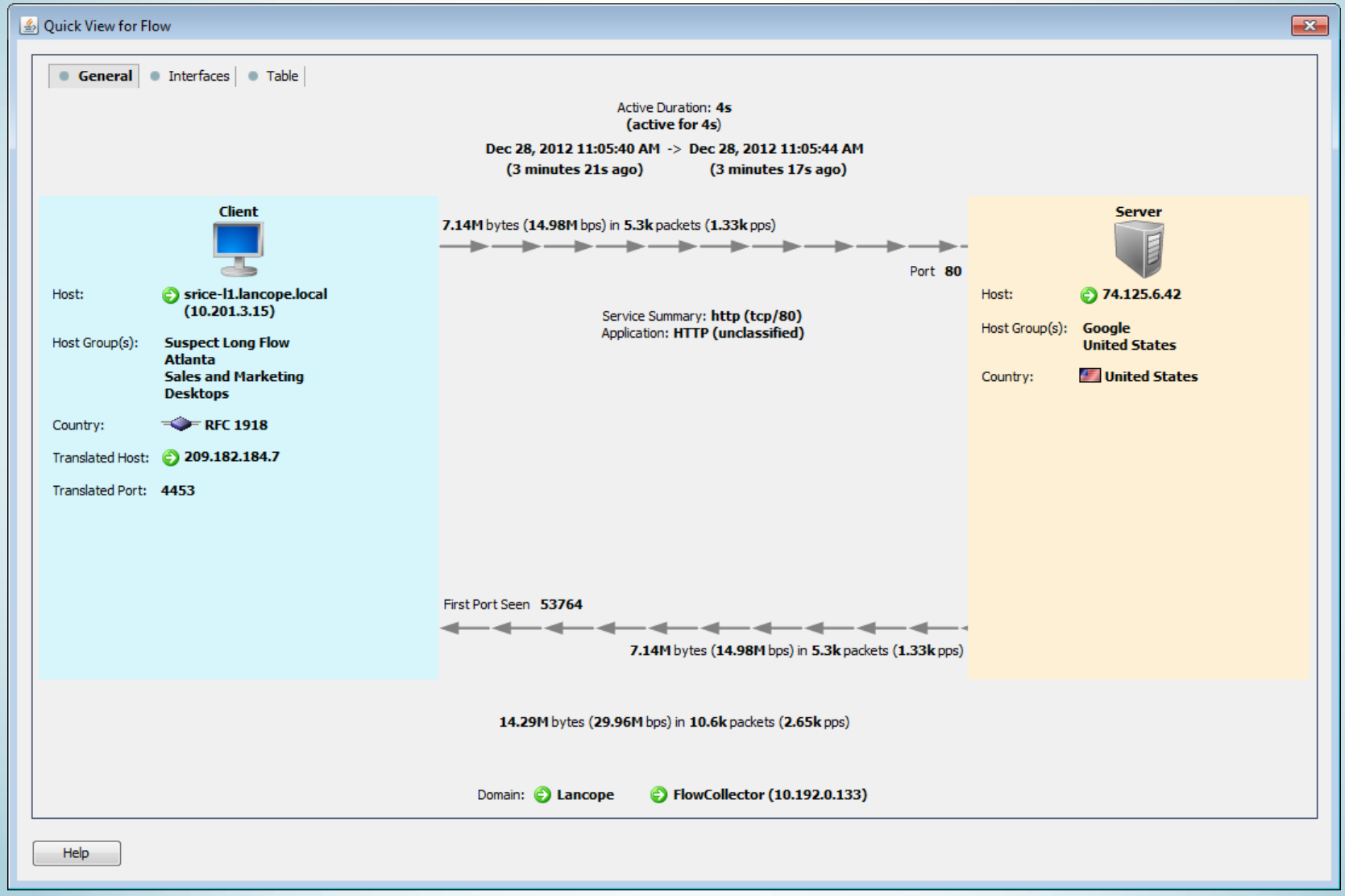


Exporter	Exporter...	Interface	Direction	TTL	DSCP	Flow Act...
10.240.200.2	Exporter	ifIndex-1	Inbound		best_effort	
10.240.200.2	Exporter	ifIndex-2	Outbound			
10.240.200.1	Cisco ASA	Wan	Inbound			Permitted
10.240.200.1	Cisco ASA	Lan	Outbound			Permitted
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan1	Outbound			
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan240	Inbound		best_effort	

Help

Stitching & De-duplication

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT



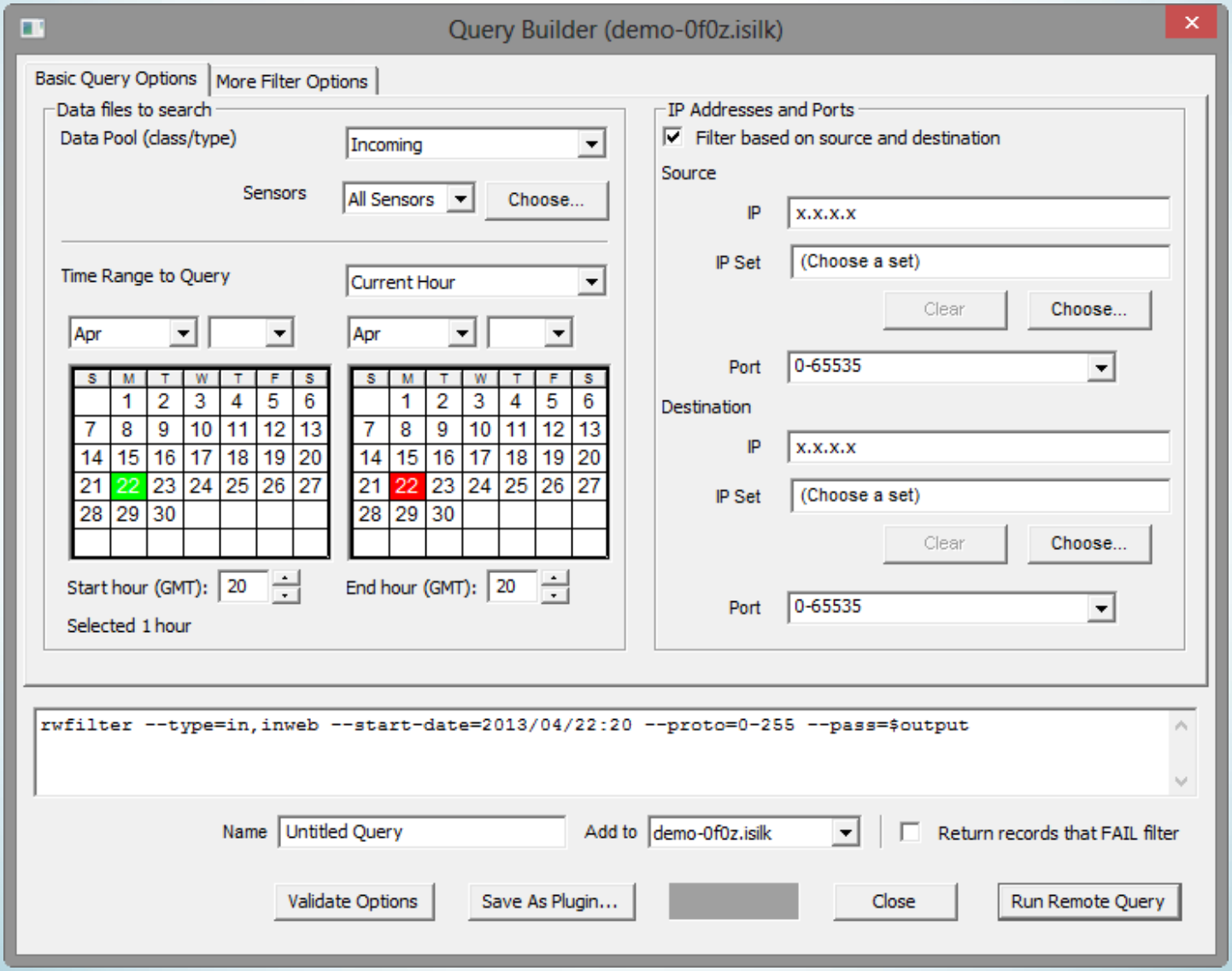
TOOLS: SILK

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

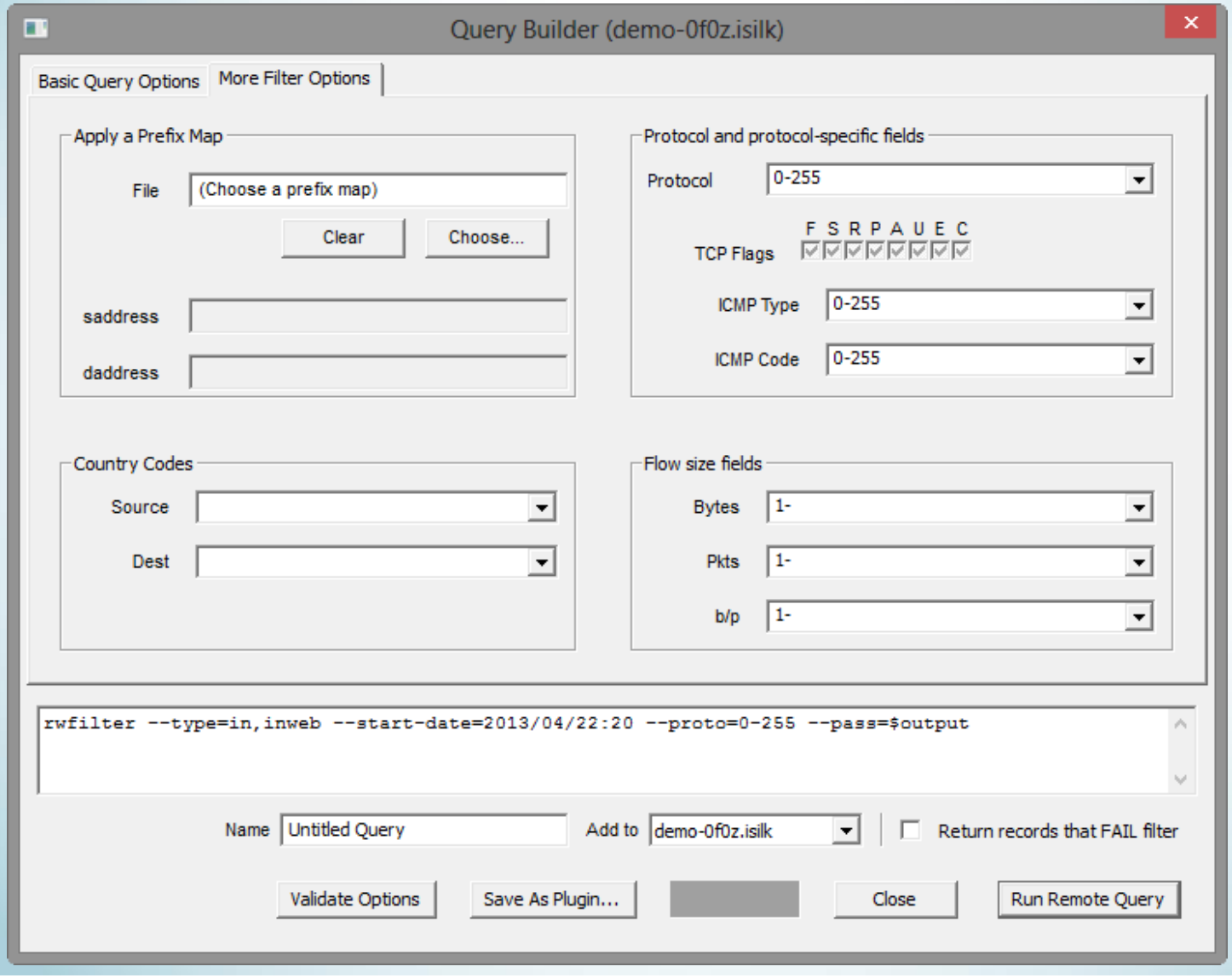
SiLK

- Download at http://tools.netsa.cert.org
- Stores and processes flow
- Project Managed by Carnegie Mellon CERT

iSiLK


Query Builder (demo-0f0z.isilk)
Basic Query Options
More Filter Options
Data files to search
Data Pool (class/type)
Incoming
Sensors
All Sensors
Choose...
Time Range to Query
Current Hour
Apr
Apr
Start hour (GMT): 20
End hour (GMT): 20
Selected 1 hour
IP Addresses and Ports
Filter based on source and destination
Source
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
0-65535
Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
0-65535
rwfilter --type=in,inweb --start-date=2013/04/22:20 --proto=0-255 --pass=$output
Name
Untitled Query
Add to
demo-0f0z.isilk
Return records that FAIL filter
Validate Options
Save As Plugin...
Close
Run Remote Query

iSiLK


Query Builder (demo-0f0z.isilk)
Basic Query Options
More Filter Options
Apply a Prefix Map
File
(Choose a prefix map)
Clear
Choose...
saddress
daddress
Protocol and protocol-specific fields
Protocol
0-255
F S R P A U E C
TCP Flags
ICMP Type
0-255
ICMP Code
0-255
Country Codes
Source
Dest
Flow size fields
Bytes
1-
Pkts
1-
b/p
1-
rwfilter --type=in,inweb --start-date=2013/04/22:20 --proto=0-255 --pass=$output
Name
Untitled Query
Add to
demo-0f0z.isilk
Return records that FAIL filter
Validate Options
Save As Plugin...
Close
Run Remote Query

PySiLK

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

```
# Import the global variables needed for processing the record
global smtpports, counts

# Pull data from the record
sip = rec.sip
bytes = rec.bytes

# Get a reference to the current data on the IP address in question
data = counts.setdefault(sip, [0, 0])

# Update the total byte count for the IP address
data[0] += bytes

# Is the flow mail related?  If so add the byte count to the mail bytes
if (rec.protocol == 6 and rec.sport in smtpports and
    rec.packets > 3 and rec.bytes > 120):
    data[1] += bytes
    return True

# If not mail related, fail the record
return False
```

Lancope.
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Commercial Solutions

- Arbor PeakFlow
- IBM Qradar
- Invea-Tech FlowMon
- Lancope StealthWatch
- ManageEngine
- McAfee NTBA
- Plixer Scrutinizer
- ProQSys FlowTraq
- Riverbed Cascade (formerly Mazu)

* For comparison see Gartner Network Behavior Analysis Market December 2012 (G00245584)

WHAT CAN LOGGING REVEAL

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Signature Matching

- Look for “known bad” conversations
- Match against data collected in NetFlow
- Per Flow Analysis

What Can Intelligent NetFlow Analysis Do?

Lancope.
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Reveal BotNet Hosts

Policy	Start Active Time	Source	Source Host Groups	Target	Target Country	Target Host Groups	Details
Inside Hosts	Feb 11, 2013 2:40:00 PM (1 hour 53 minutes 27s ago)	209.182.184.8	Atlanta	ns1.dns-domainserve (82.208.40.4)	Czech Republic	Czech Republic, Zeus	Successful communication was detected between this inside host and C&C server using port 80 and the TCP protocol, and http://host1.fileserv.uni.me/css...

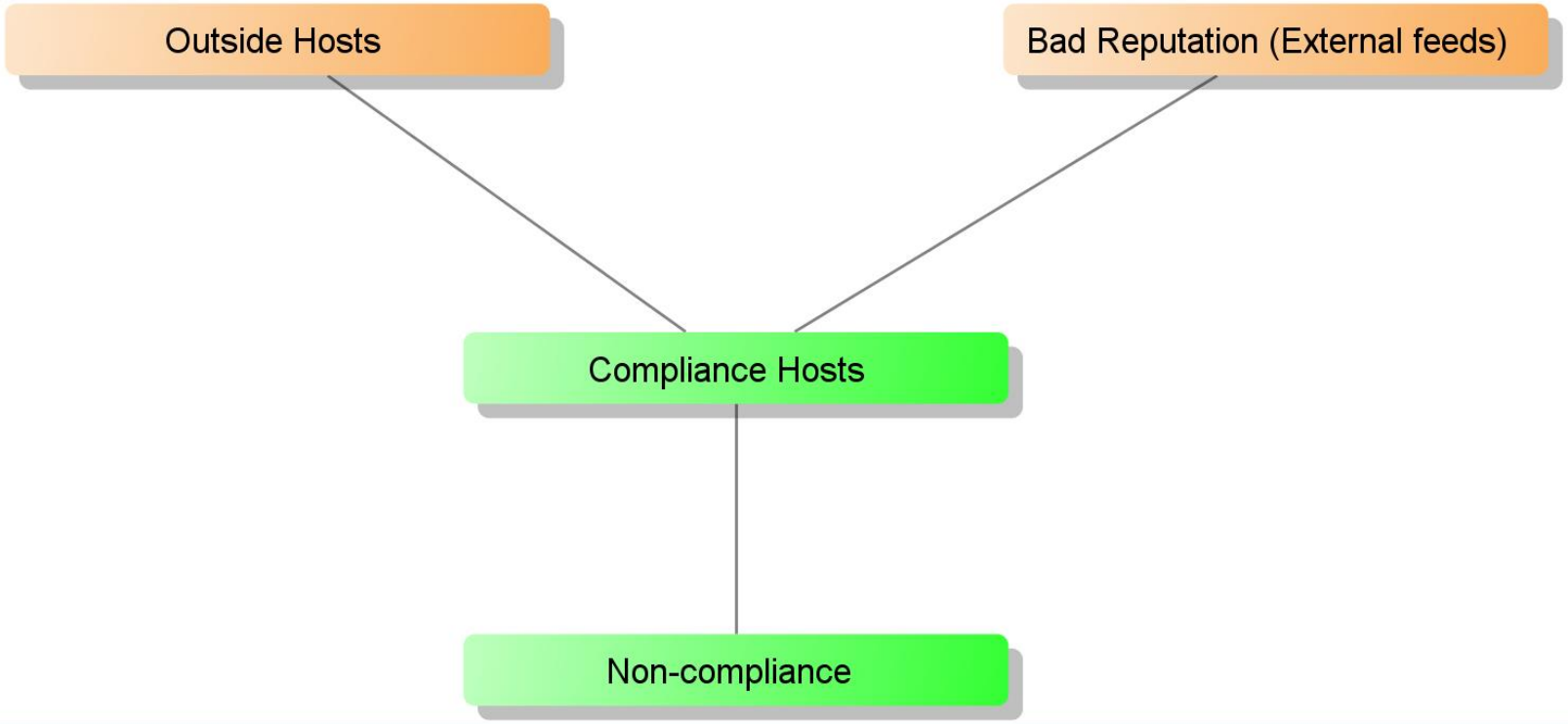
Layer 3

Layer 4 and URL

What Can Intelligent NetFlow Analysis Do?

Lancope.
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Report on Compliance

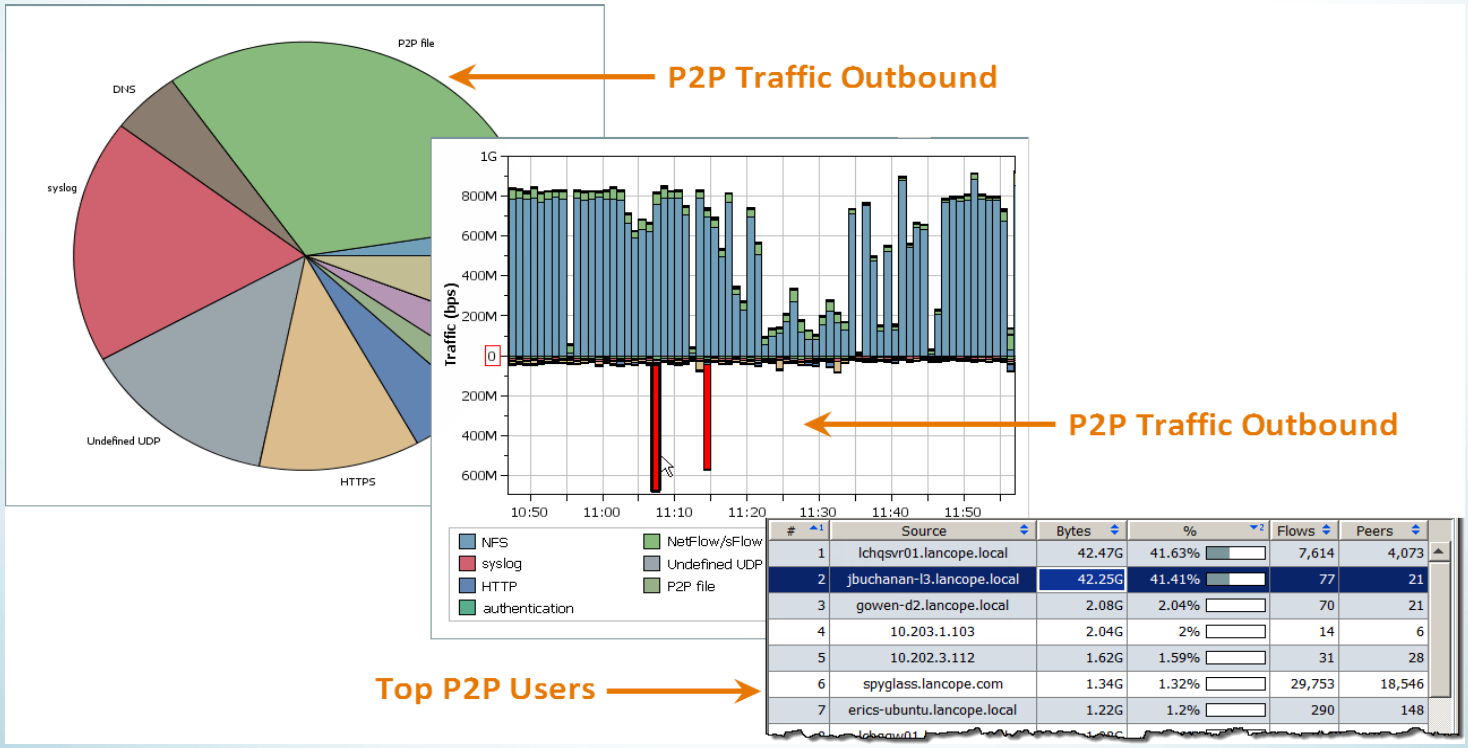


What Can Intelligent NetFlow Analysis Do?

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Unsanctioned Device and Application Detection

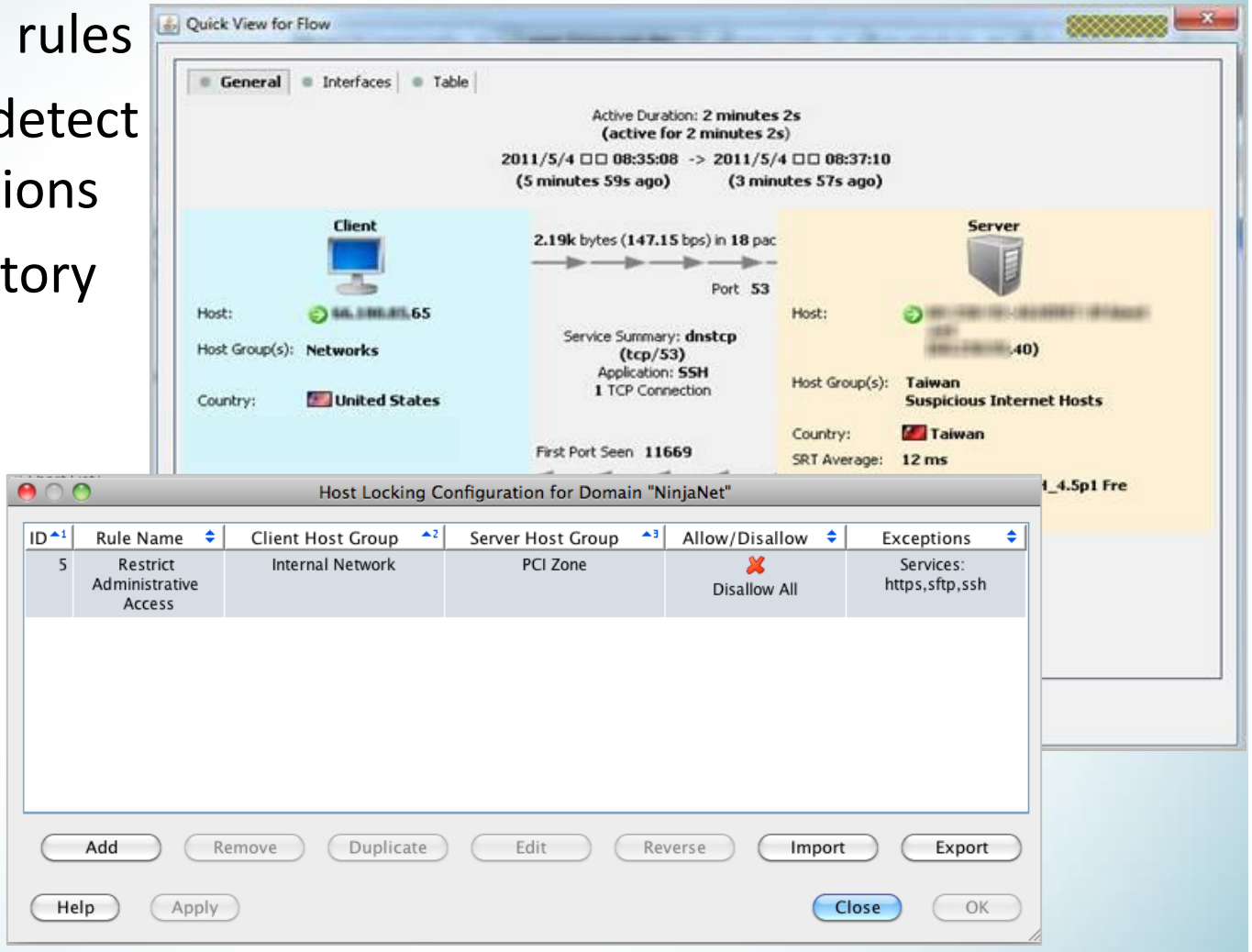
- Identify the use of unsanctioned applications
- Detect rogue servers and other rogue devices



What Can Intelligent NetFlow Analysis Do?

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

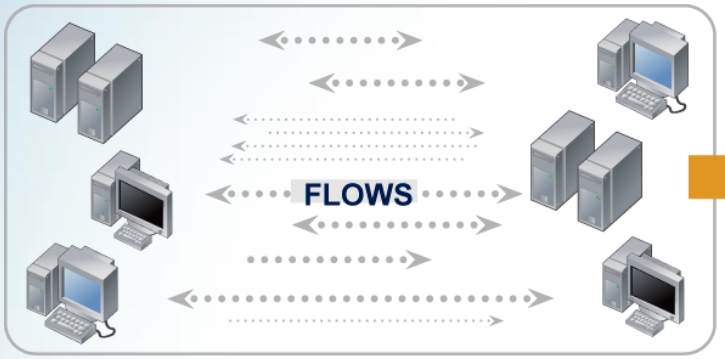
- Audit Firewall rules
- Immediately detect misconfigurations
- Ensure regulatory compliance



Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Behavior-based Analysis of Network Flows

Collect and analyze flows

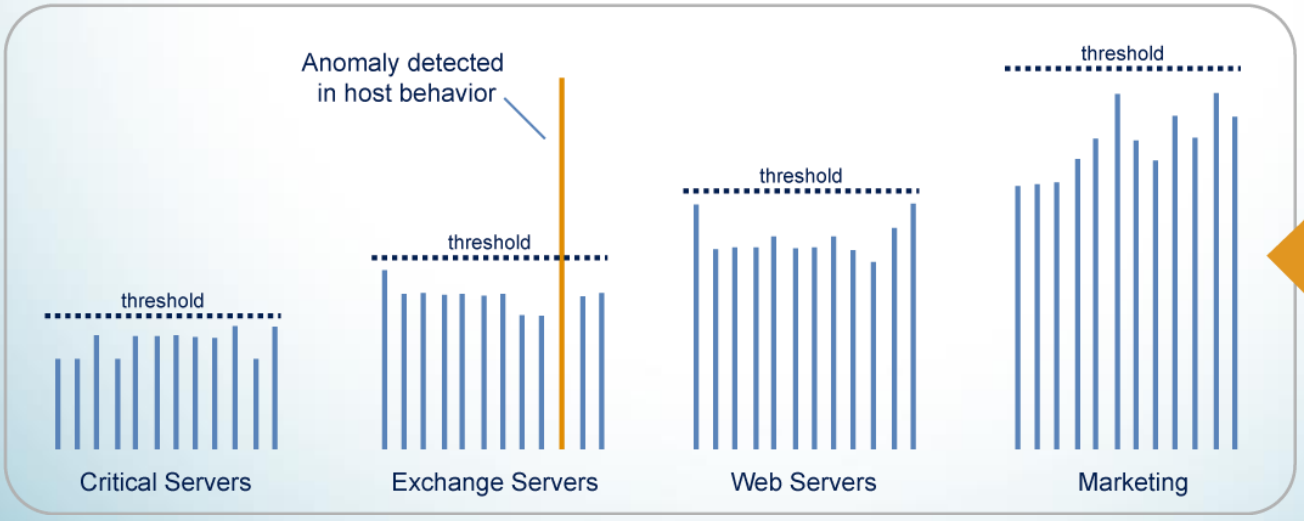


Establish baseline of behavior

BEHAVIOR

- Number of concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of Syns received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Alarm on anomalies and changes in behavior



What Can Intelligent NetFlow Analysis Do?

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Reveal Recon

Internal Spreading Malware | Bot Detection | Suspect Data Loss | Policy Violation | Reconnaissance Detection | DDoS Detection | Alarms

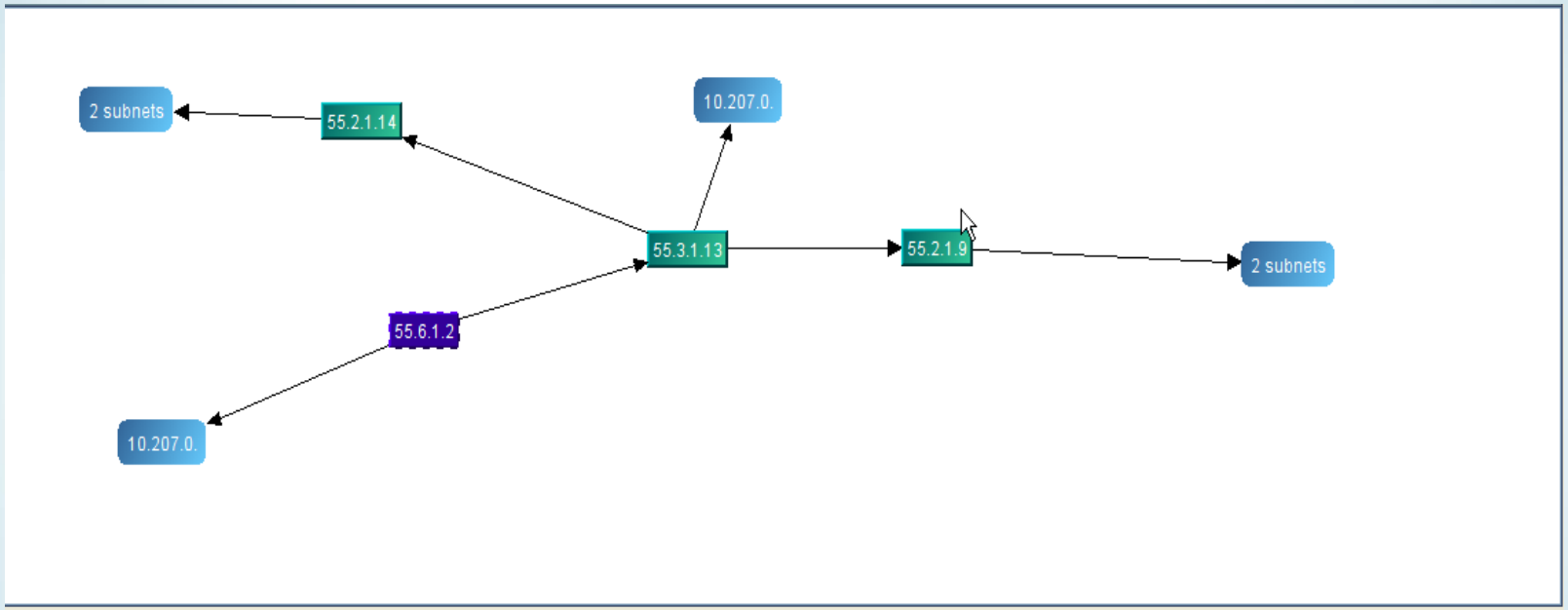
Concern Index - 16 records summarized into 16 records

Host Groups	Host	CI	CI%	Alerts
Atlanta	spyglass.lancope.com (209.182.184.2)	3,520,636	1,174%	Excess_Clients, Port_Scan
Atlanta	209.182.184.1	26,888,520	269%	Rejects, UDP_Scan
Sales and Marketing, Atlanta, Users, Windows	jbuchanan-d2.lancope.local (10.201.3.24)	15,995,525	160%	TCP_Scan
New York, Windows	10.90.10.254	9,132,249	91%	TCP_Scan
New York, Windows	10.30.10.254	8,312,191	83%	TCP_Scan
New York, Windows	10.40.10.254	8,329,626	83%	TCP_Scan
New York, Windows	10.80.10.254	8,344,656	83%	TCP_Scan
New York, Windows	10.70.10.254	8,182,332	82%	TCP_Scan
New York, Windows	10.50.10.254	8,074,116	81%	TCP_Scan
New York, Windows	10.100.10.254	8,020,008	80%	TCP_Scan
New York, Windows	10.20.10.254	7,686,342	77%	TCP_Scan
New York	10.110.10.254	7,608,186	76%	TCP_Scan
New York, Windows	10.60.10.254	7,202,376	72%	TCP_Scan
Atlanta	209.182.176.42	2,144,863	67%	Rejects
SG Private	lcsgfw01.lancope.local (10.192.0.1)	5,972,924	60%	Ping, Ping_Oversized_Packet, Ping_Scan, Rejects
Sales and Marketing, Atlanta, Users, Windows	10.201.3.83	5,903,806	59%	Ping_Oversized_Packet, TCP_Scan

What Can Intelligent NetFlow Analysis Do?

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Investigate Infections



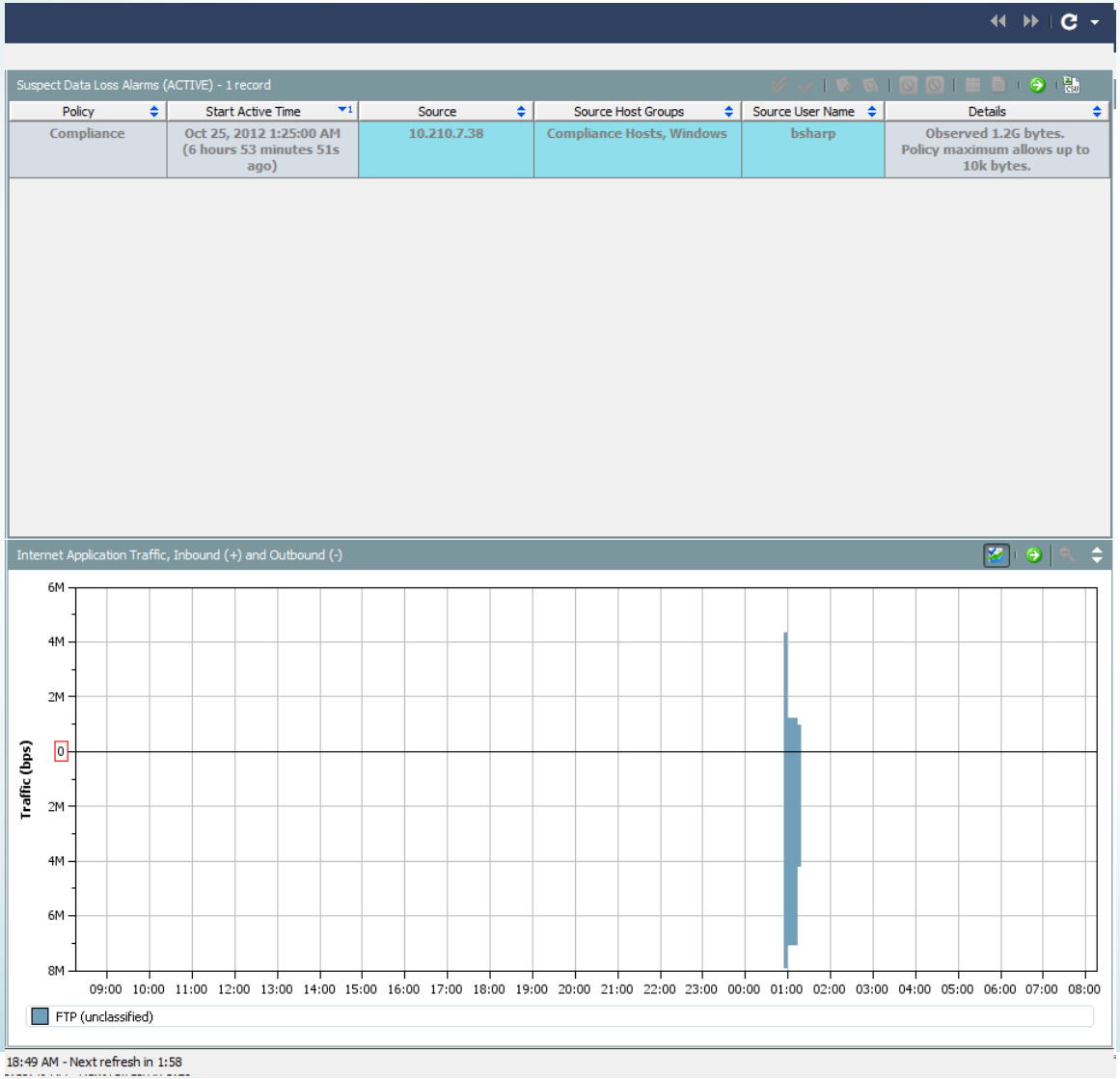
Details - 2 records

Earliest Time	Port	Protocol	Next Hop	Total Hosts Subnet	Propagated Hosts Subnet
05/22/08 01:15:59	445	tcp	55.3.1.13	3	17
05/22/08 01:16:09	445	tcp	Subnet 10.207.0.	1	

What Can Intelligent NetFlow Analysis Do?

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Loss of Protected Data

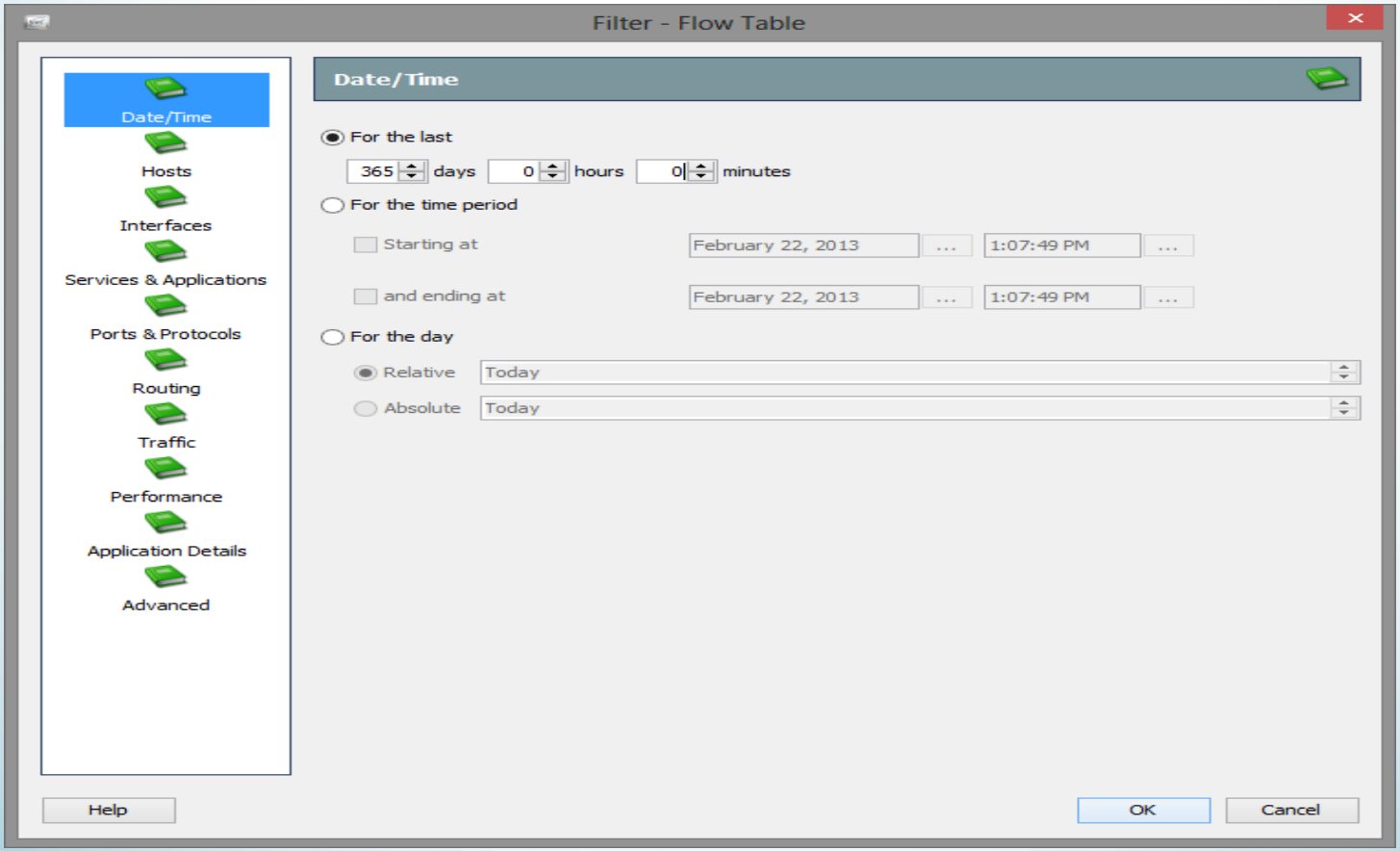


FORENSIC INVESTIGATIONS

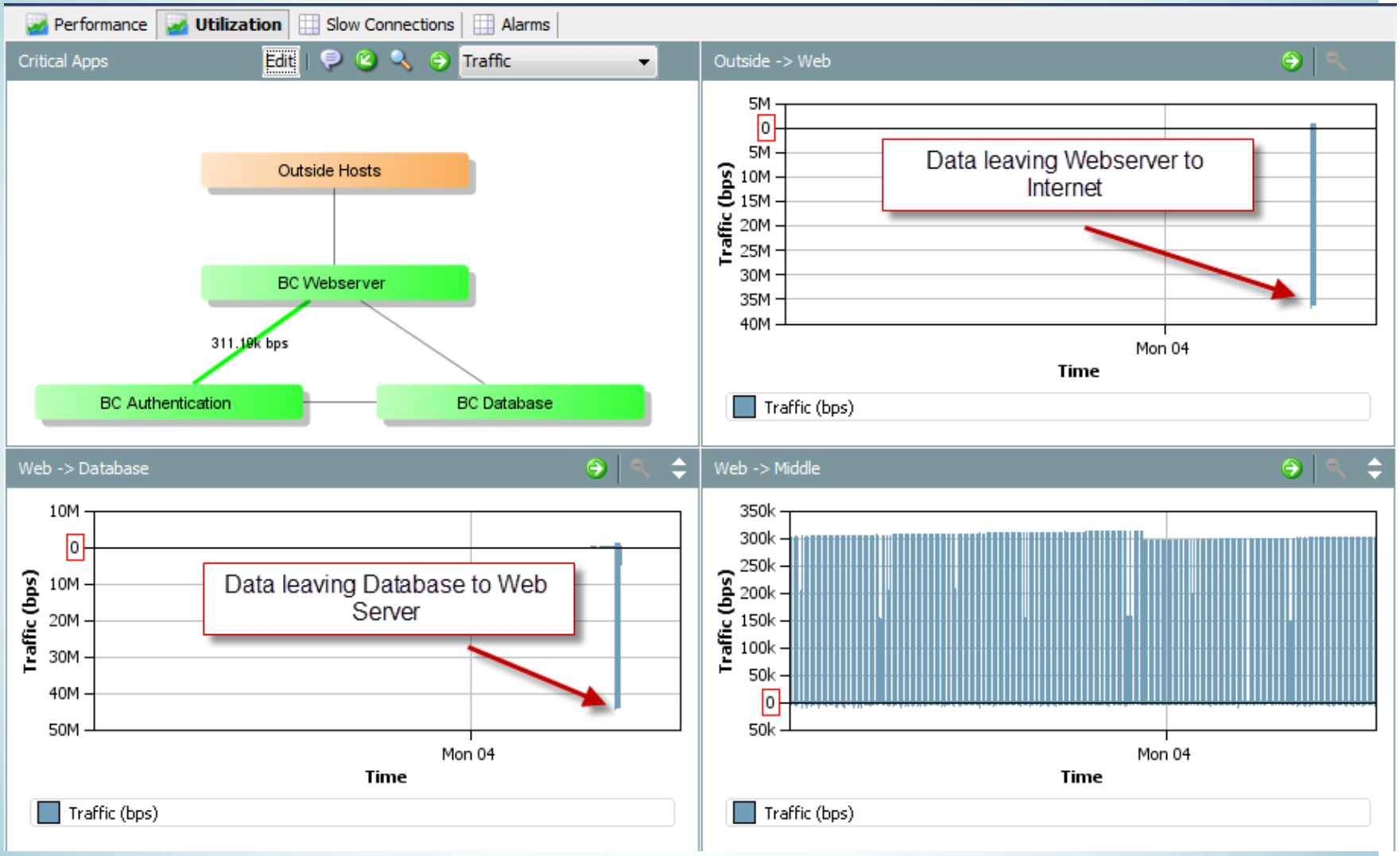
Forensic Q&A

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

How long has behavior been active? Historical Traffic Report
Which hosts have a compromised host "touched?" Top Peers (filtered to Internal or Critical)
Has this attack happened in the past? Flow Table on available data points
How long has this attacker been lurking around the network? Historical Traffic on Host



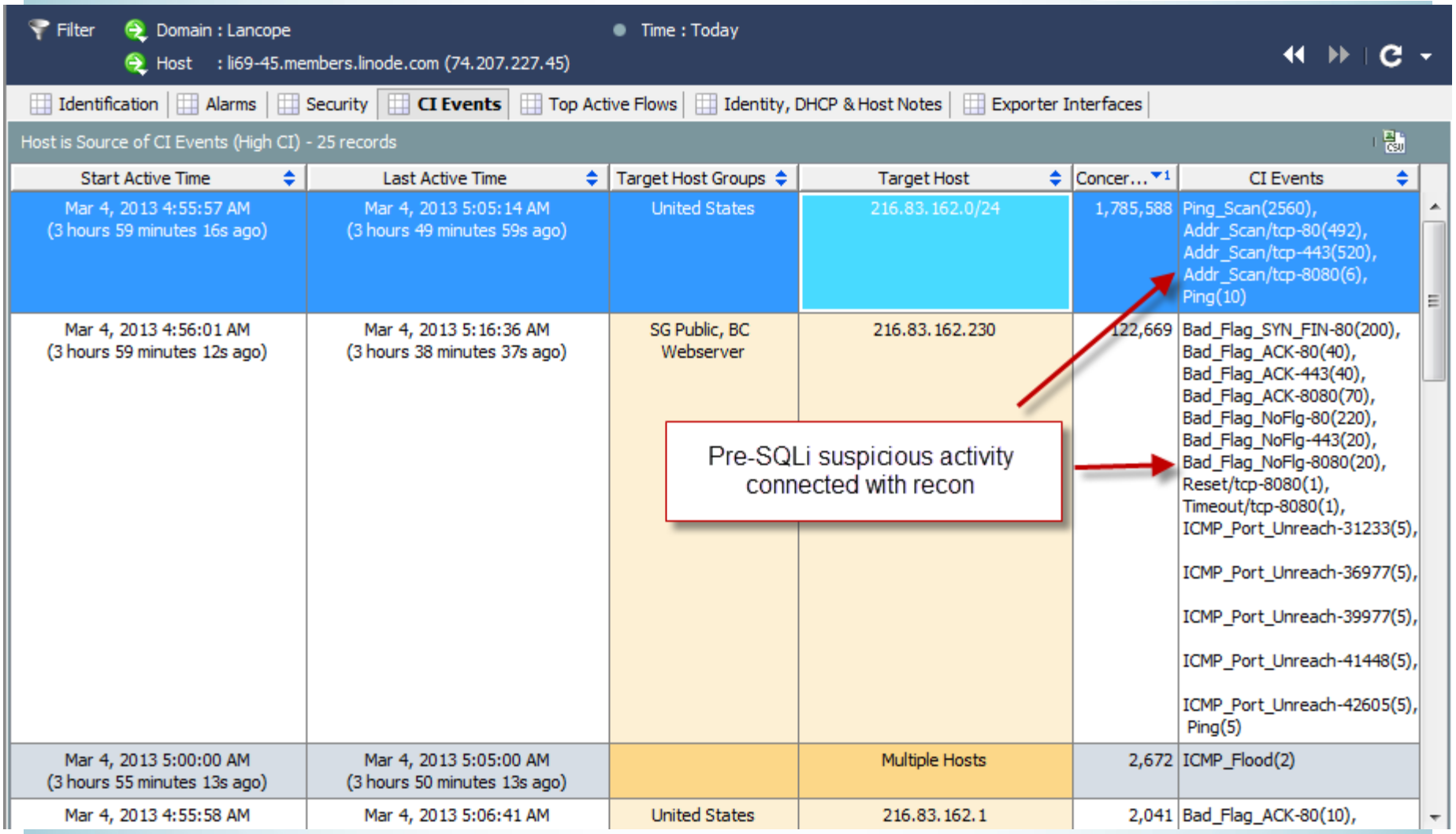
SQL Injection



SQL Injection

SQL Injection

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

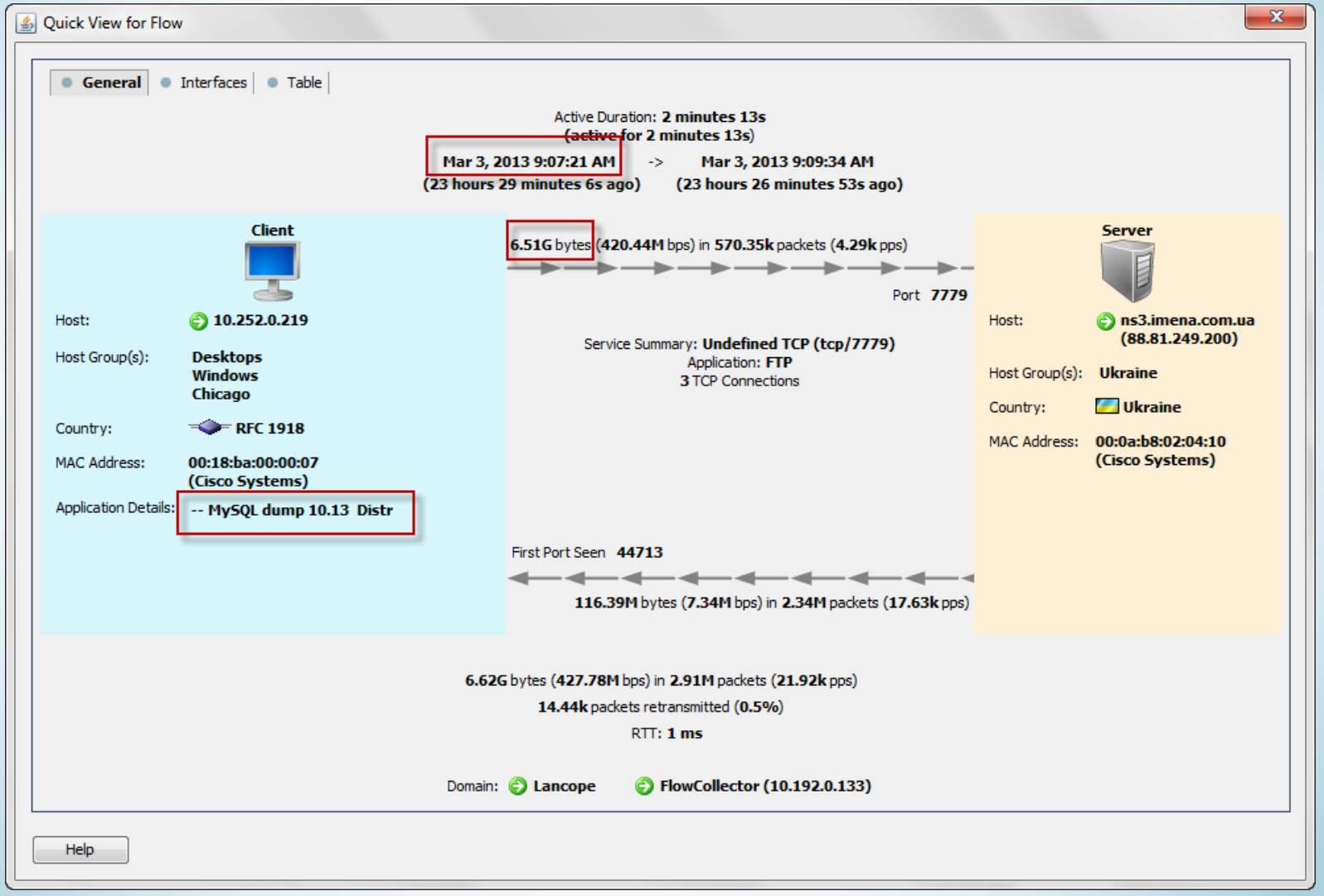


Beron's abnormal disclosure

Policy	Start Active T...	Alarm	Source	Source Host Gr...	Source U...	Target	Target H...	Details
Compliance Hosts	Mar 3, 2013 7:35:00 AM (1 day 1 hour ago)	Suspect Data Loss	10.210.7.38	Control Servers, Windows	lucy	Multiple Hosts		Observed 2.41G bytes. Policy maximum allows up to 1k bytes.
Inside Hosts	Mar 3, 2013 9:15:00 AM (23 hours 20 minutes 48s ago)	Suspect Data Loss	10.252.0.219	Desktops, Windows, Chicago	beron	Multiple Hosts		Observed 8.28G bytes. Policy maximum allows up to 500M bytes.

Abnormal Data Upload

What did Beron send? Who received it?



Where could have Beron gotten the data?

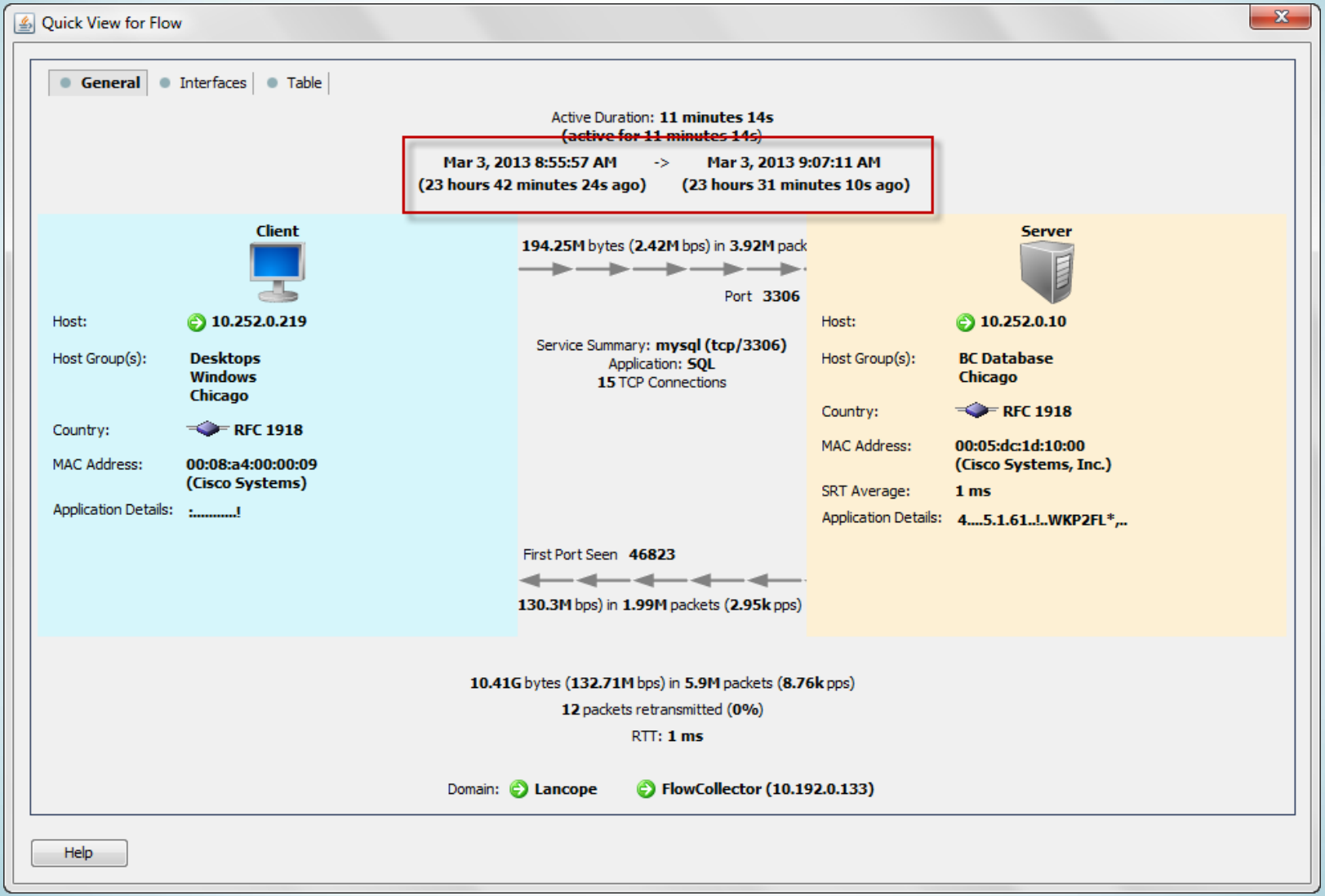
Filter
Domain : Lancope
Client Host : 10.252.0.219
Server Host Group : Inside Hosts
Direction : Total
Time : Last 1 day

Top Peers - 2 records

.	% of Bytes	Peer	Peer Host Groups	Peer Role	Average Traffic (b...	Bytes	Flows	Hosts	Peer Bytes Ratio
1	10...	10.252.0.10	BC Database, Chicago	Server	114.68M	10.41G	1	1	98.18%
	10...	Total (1)		Server	114.68M	10.41G	1	1	98.18%

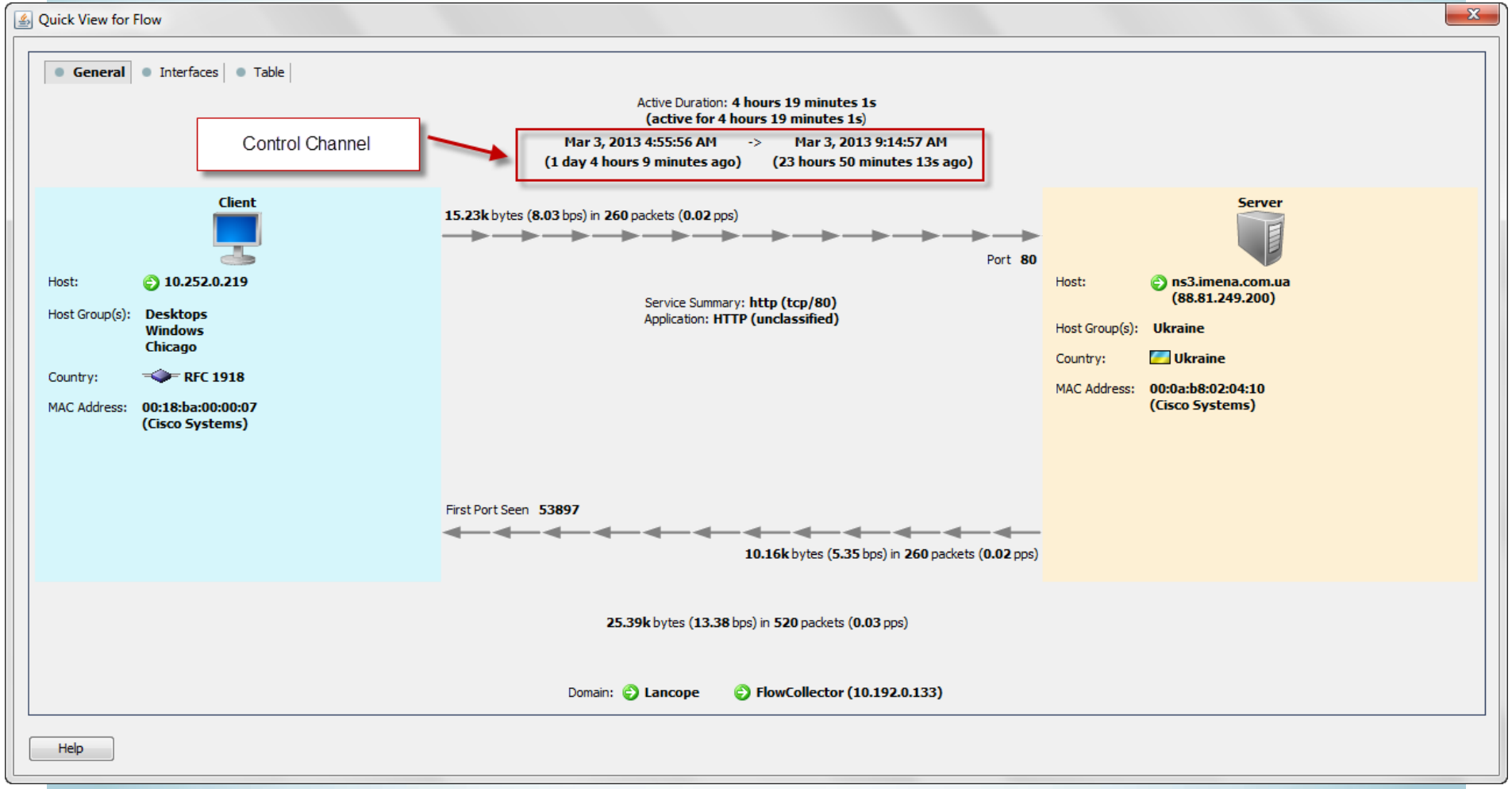
Data Theft

Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT



Lancope
VISION TO SECURE,
INTELLIGENCE TO PROTECT

Why did Beron do it?



Lancope.
VISION TO SECURE,
INTELLIGENCE TO PROTECT

- **Web**
  www.lancope.com (Company)
  f15h.co (Personal)

- **Twitter**
  @Lancope (Company)
  @netflowninjas (Company Blog)
  @charlesherring (Personal)

- **Charles Herring**
  Sr. Systems Engineer, Lancope
  cherring@lancope.com