COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Network mgmt tools

keeping the free love alive

Alan Crosswell
alan@columbia.edu

COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Credits

- Dan Medina
- Matt Selsky
- Megan Pengelly
- Martin Wren
- Johan Anderson
- Joel Rosenblatt
- + all the GPL tool authors

Outline

- Network management
  - Switch management
  - Router configs
  - Log summarization
  - Netflow
  - Survivor systems monitor
  - Intermapper

Outline

- Security
  - GULP – auth log mining
  - PAIRS – IDS
  - Mazu – anomaly detection

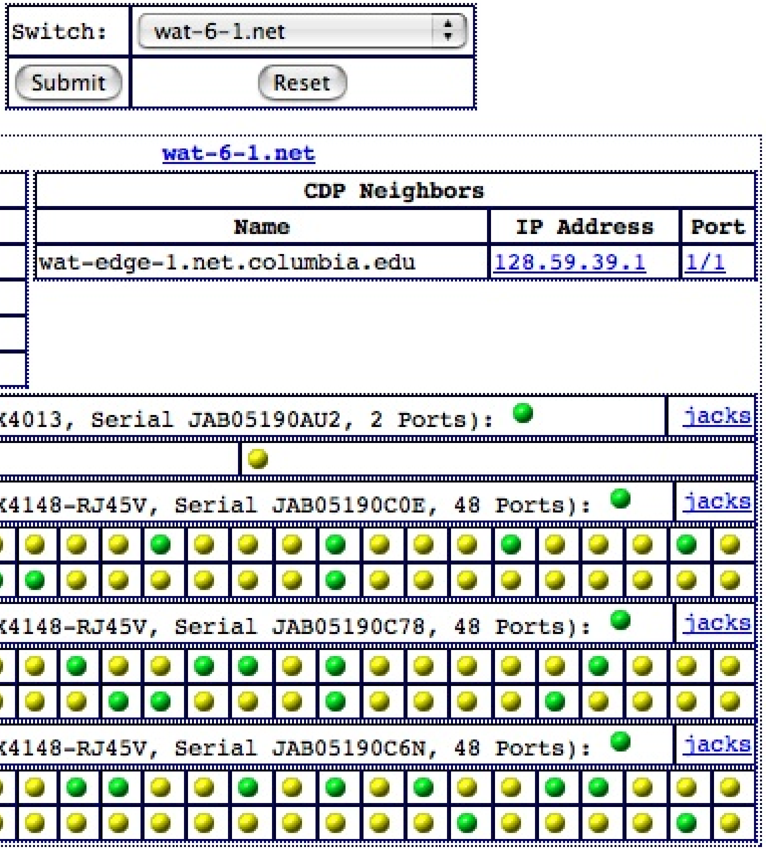
Switchmgr

- Web interface to SNMP commands to Cisco CatOS/IOS switches/routers on campus
- Database backend provides another layer of information for ports:
  - Jack location information <-> port number
  - (LDAP) jack location <-> person

Switchmgr Privileges

- Use pamacea to authenticate users
- Users view/modify switches based on their Unix groups
  - Student RCCs can only view dorm switches
  - Cabling group can only modify jack location information

Switchmgr: switch view



Switch:	wat-6-1.net
Submit	Reset

wat-6-1.net

Legend	
🟢	Connected
🟡	Not Connected
🔴	Disabled
🔵	Major Fault
⚪	Unknown

CDP Neighbors

Name	IP Address	Port
wat-edge-1.net.columbia.edu	128.59.39.1	1/1

Module 1 (Model WS-X4013, Serial JAB05190AU2, 2 Ports): 🟢 jacks

🟢	🟡

Module 2 (Model WS-X4148-RJ45V, Serial JAB05190C0E, 48 Ports): 🟢 jacks

🟢	🟢	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟢	🟡
🟡	🟡	🟡	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡

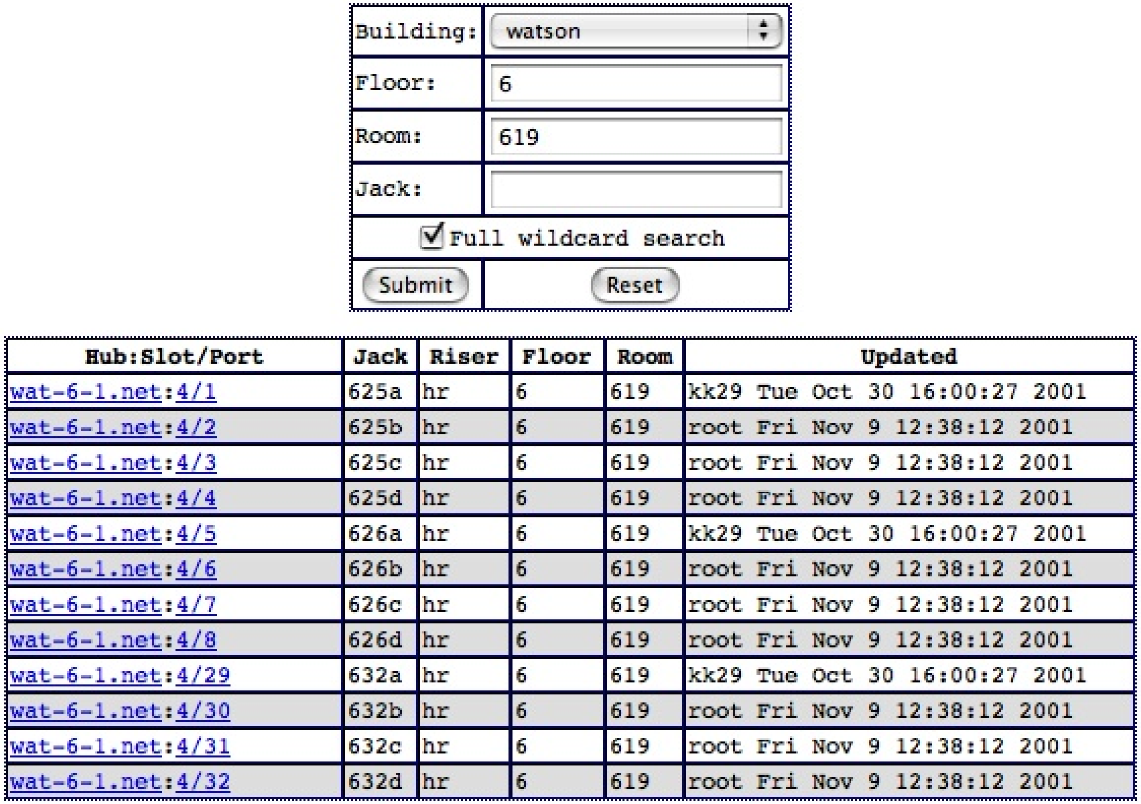
Module 3 (Model WS-X4148-RJ45V, Serial JAB05190C78, 48 Ports): 🟢 jacks

🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟡
🟡	🟡	🟡	🟢	🟡	🟢	🟡	🟡	🟡	🟢	🟢	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟡

Module 4 (Model WS-X4148-RJ45V, Serial JAB05190C6N, 48 Ports): 🟢 jacks

🟡	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🟢	🟢	🟡	🟡	🟢	🟡	🟢	🟡	🟢	🟡	🟡	🟢	🟢	🟡	🟡	🟡
🟡	🟢	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟡	🟡	🟢	🟡

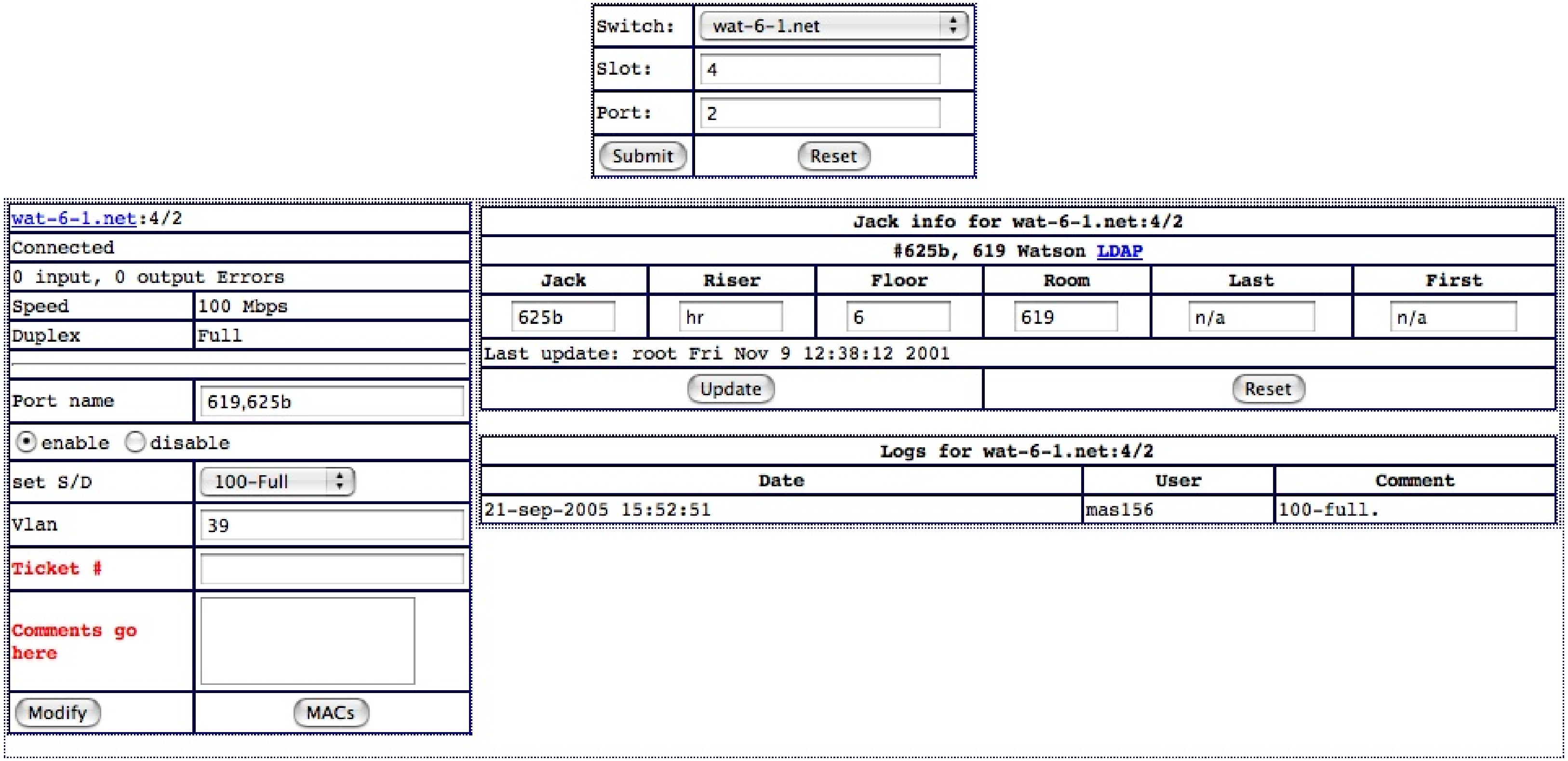
Switchmgr: jack view



Building:	watson
Floor:	6
Room:	619
Jack:	
☑ Full wildcard search	
Submit	Reset

Hub:Slot/Port	Jack	Riser	Floor	Room	Updated
wat-6-1.net:4/1	625a	hr	6	619	kk29 Tue Oct 30 16:00:27 2001
wat-6-1.net:4/2	625b	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/3	625c	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/4	625d	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/5	626a	hr	6	619	kk29 Tue Oct 30 16:00:27 2001
wat-6-1.net:4/6	626b	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/7	626c	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/8	626d	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/29	632a	hr	6	619	kk29 Tue Oct 30 16:00:27 2001
wat-6-1.net:4/30	632b	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/31	632c	hr	6	619	root Fri Nov 9 12:38:12 2001
wat-6-1.net:4/32	632d	hr	6	619	root Fri Nov 9 12:38:12 2001

Switchmgr: port view



Switch:	wat-6-1.net
Slot:	4
Port:	2
Submit	Reset

wat-6-1.net:4/2	
Connected	
0 input, 0 output Errors	
Speed	100 Mbps
Duplex	Full
Port name	619,625b
● enable ○ disable	
set S/D	100-Full
Vlan	39
Ticket #	
Comments go here	
Modify	MACs

Jack info for wat-6-1.net:4/2

#625b, 619 Watson LDAP

Jack	Riser	Floor	Room	Last	First
625b	hr	6	619	n/a	n/a

Last update: root Fri Nov 9 12:38:12 2001

Update   Reset

Logs for wat-6-1.net:4/2

Date	User	Comment
21-sep-2005 15:52:51	mas156	100-full.

Cisco Config Management

- Nightly backups into RCS to archive all switch and router configs
- Currently uses 'clogin' from RANCID project to authenticate and run automatically
- Web-based comparison tool for viewing changes to configs over time, or can just use RCS at the command-line
- Nightly email tells group which switches & routers have changed their configurations since the previous day

Switch & Router Log Monitoring

- cisco-summary.pl emails log summaries to our group every day
- Person On Call ensures that all log messages are OK, or fixes any problems found

Netflow

- Track traffic going across the border
- CFlowd on a linux machine to process flow files exported from main routers
- CUFlow builds on Cflow tools to provide graphs and charts per service or router
- CUQuota monitors bytes to and from internal hosts and polices them when they exceed 180 M/h upload or 350 M/h download

CUFlow

- Our graphing/charting Cflow class is GPL'd and available at

- http://www.columbia.edu/acis/networks/advanced/CUFlow

Survivor

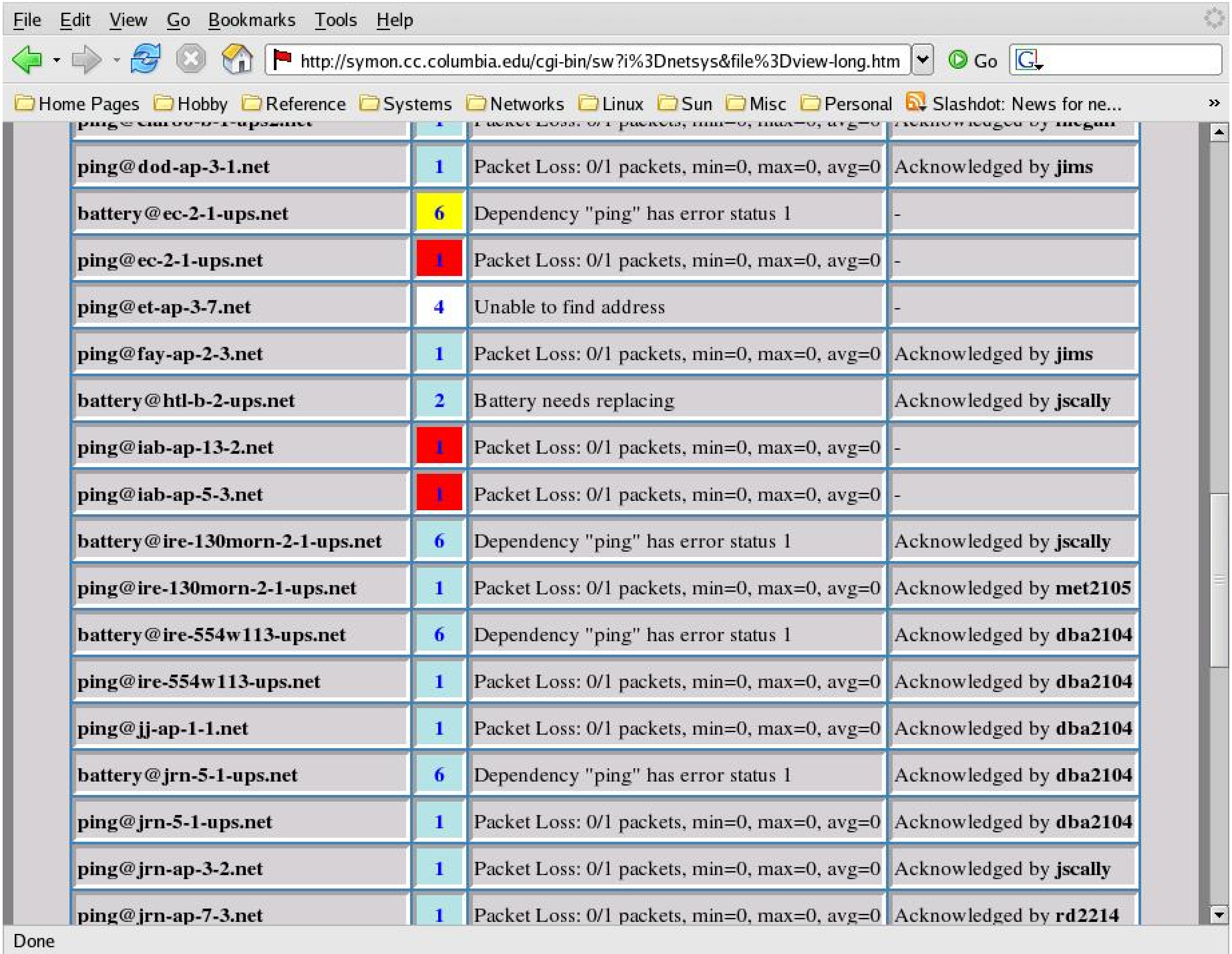
- "It's a systems monitor. It monitors systems." Like Mon, Big Brother, Nagios, etc, but better or worse, depending on what features you like.
- http://freshmeat.net/projects/survivor/
- demo

```
# This file is used to configure the filesystem checking on
each host.
# The format of this file is
#   filesysregex,warn,prob
# Disks not explicitly listed here use the default thresholds
in check.cf.
# Disks listed here that don't exist are ignored.
# Values must be greater than 0.  101 or greater will never
match, and so
# can be used to suppress warnings or problems.
#
# Important filesystems should have some spare space
^/$,90,94
# Some hosts write variable stuff into /var, others /usr/var
^/usr$,90,94
^/var$,90,94
# Generate warnings, but not problems, for filesystems
holding software
^/usr/local,98,101
^/opt,98,101
^/miniopt,98,101
^/service,98,101
# Some filesystems are never worth worrying about
^/m/mnt,101,101
...
```

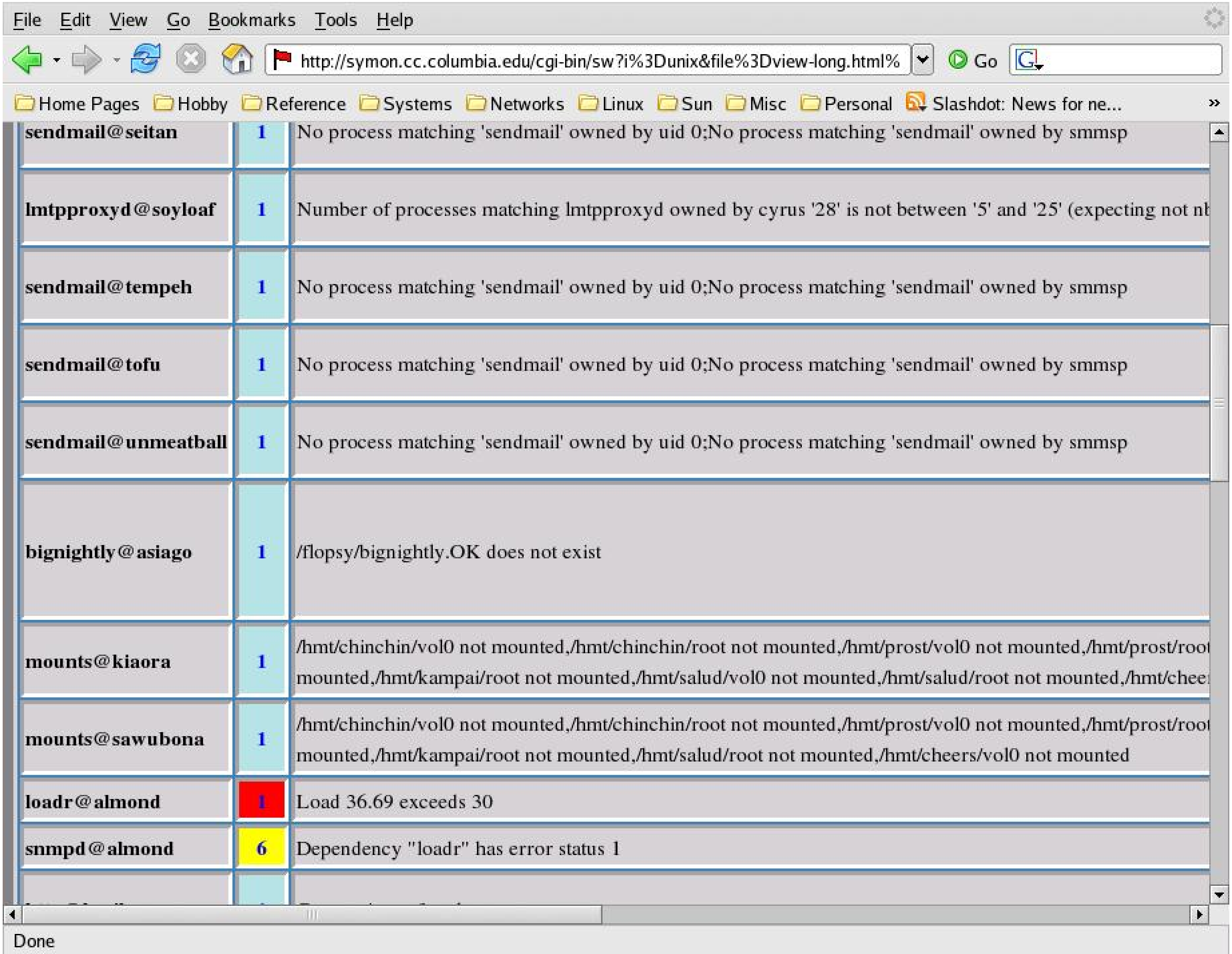
```
# Survivor check specification file
check load {
  module load {
    warn 20
    prob 30
  }
}
check loadna {
  module snmp {
    community XXX
    oid        .iso.3.6.1.4.1.789.1.2.1.3.0
    warnmatch gt[75]
    probmatch gt[90]
  }

  alert on noncritical alertplan
}
check ldapmain {
  module ldap {
    port    389
    filter  sn=metz
    response objectclass=person
  }

  helpfile ldapmain
}
```


File Edit View Go Bookmarks Tools Help
http://symon.cc.columbia.edu/cgi-bin/sw?i%3Dnetsys&file%3Dview-long.htm
Go
Home Pages
Hobby
Reference
Systems
Networks
Linux
Sun
Misc
Personal
Slashdot: News for ne...
Done

ping@clar86-b-1-ups2.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **megan**
ping@dod-ap-3-1.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **jims**
battery@ec-2-1-ups.net	6	Dependency "ping" has error status 1	-
ping@ec-2-1-ups.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	-
ping@et-ap-3-7.net	4	Unable to find address	-
ping@fay-ap-2-3.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **jims**
battery@htl-b-2-ups.net	2	Battery needs replacing	Acknowledged by **jscally**
ping@iab-ap-13-2.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	-
ping@iab-ap-5-3.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	-
battery@ire-130morn-2-1-ups.net	6	Dependency "ping" has error status 1	Acknowledged by **jscally**
ping@ire-130morn-2-1-ups.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **met2105**
battery@ire-554w113-ups.net	6	Dependency "ping" has error status 1	Acknowledged by **dba2104**
ping@ire-554w113-ups.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **dba2104**
ping@jj-ap-1-1.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **dba2104**
battery@jrn-5-1-ups.net	6	Dependency "ping" has error status 1	Acknowledged by **dba2104**
ping@jrn-5-1-ups.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **dba2104**
ping@jrn-ap-3-2.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **jscally**
ping@jrn-ap-7-3.net	1	Packet Loss: 0/1 packets, min=0, max=0, avg=0	Acknowledged by **rd2214**



File Edit View Go Bookmarks Tools Help
http://symon.cc.columbia.edu/cgi-bin/sw?i%3Dunix&file%3Dview-long.html%
Go
Home Pages
Hobby
Reference
Systems
Networks
Linux
Sun
Misc
Personal
Slashdot: News for ne...
Done

sendmail@seitan	1	No process matching 'sendmail' owned by uid 0;No process matching 'sendmail' owned by smmsp
lmtpproxyd@soyloaf	1	Number of processes matching lmtpproxyd owned by cyrus '28' is not between '5' and '25' (expecting not nb
sendmail@tempeh	1	No process matching 'sendmail' owned by uid 0;No process matching 'sendmail' owned by smmsp
sendmail@tofu	1	No process matching 'sendmail' owned by uid 0;No process matching 'sendmail' owned by smmsp
sendmail@unmeatball	1	No process matching 'sendmail' owned by uid 0;No process matching 'sendmail' owned by smmsp
bignightly@asiago	1	/flopsy/bignightly.OK does not exist
mounts@kiaora	1	/hmt/chinchin/vol0 not mounted,/hmt/chinchin/root not mounted,/hmt/prost/vol0 not mounted,/hmt/prost/root mounted,/hmt/kampai/root not mounted,/hmt/salud/vol0 not mounted,/hmt/salud/root not mounted,/hmt/chee
mounts@sawubona	1	/hmt/chinchin/vol0 not mounted,/hmt/chinchin/root not mounted,/hmt/prost/vol0 not mounted,/hmt/prost/root mounted,/hmt/kampai/root not mounted,/hmt/salud/root not mounted,/hmt/cheers/vol0 not mounted
loadr@almond	1	Load 36.69 exceeds 30
snmpd@almond	6	Dependency "loadr" has error status 1

Outline

- Security
  - GULP – auth log mining
  - PAIRS – IDS
  - Mazu – anomaly detection

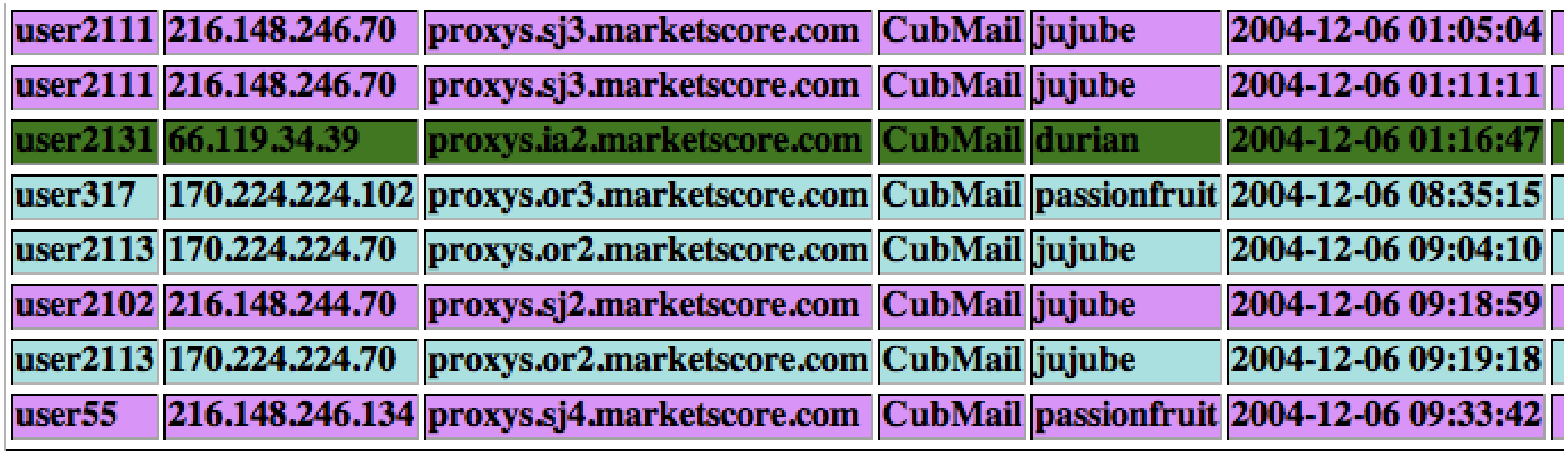
GULP

- Authn syslogs are collected in a database.
  - user identity
  - service/server
  - client IP address
- Merged with
  - MAC addresses (ARP tables polled)
  - RADIUS caller ID for dialups

GULP

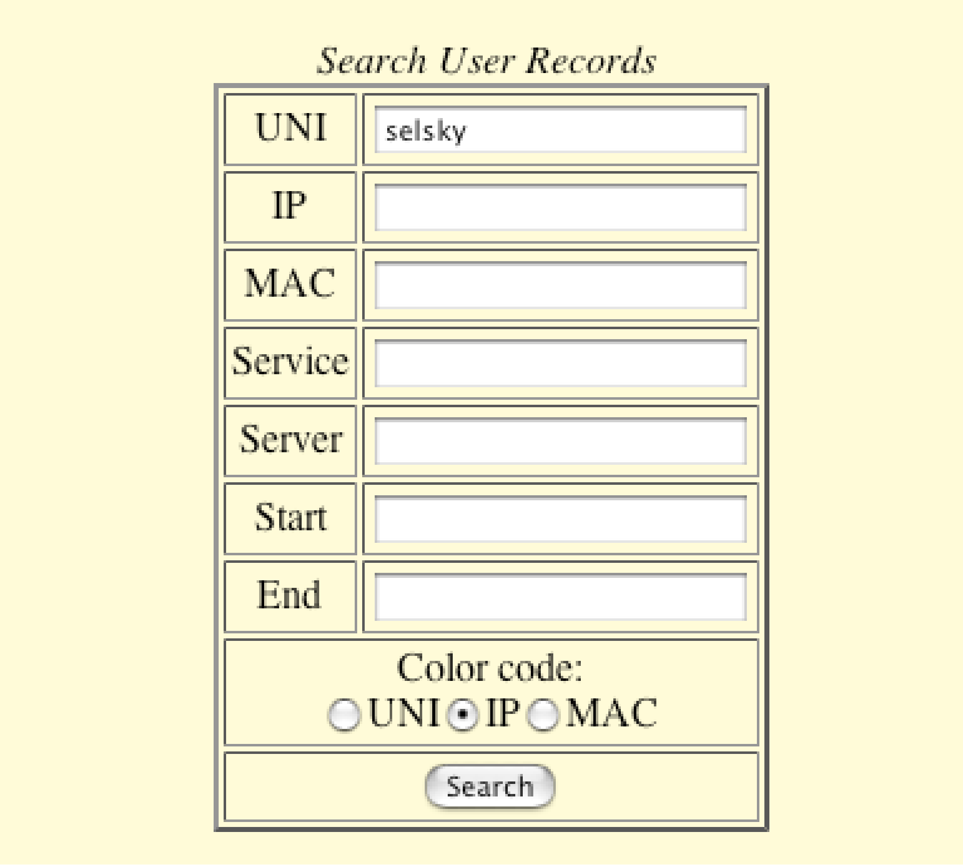
- Web interface allows searching by
  - IP addr
  - MAC addr
  - user identity
  - etc.
- demo

GULP - Marketscore



user2111	216.148.246.70	proxys.sj3.marketscore.com	CubMail	jujube	2004-12-06 01:05:04
user2111	216.148.246.70	proxys.sj3.marketscore.com	CubMail	jujube	2004-12-06 01:11:11
user2131	66.119.34.39	proxys.ia2.marketscore.com	CubMail	durian	2004-12-06 01:16:47
user317	170.224.224.102	proxys.or3.marketscore.com	CubMail	passionfruit	2004-12-06 08:35:15
user2113	170.224.224.70	proxys.or2.marketscore.com	CubMail	jujube	2004-12-06 09:04:10
user2102	216.148.244.70	proxys.sj2.marketscore.com	CubMail	jujube	2004-12-06 09:18:59
user2113	170.224.224.70	proxys.or2.marketscore.com	CubMail	jujube	2004-12-06 09:19:18
user55	216.148.246.134	proxys.sj4.marketscore.com	CubMail	passionfruit	2004-12-06 09:33:42

GULP – search for user

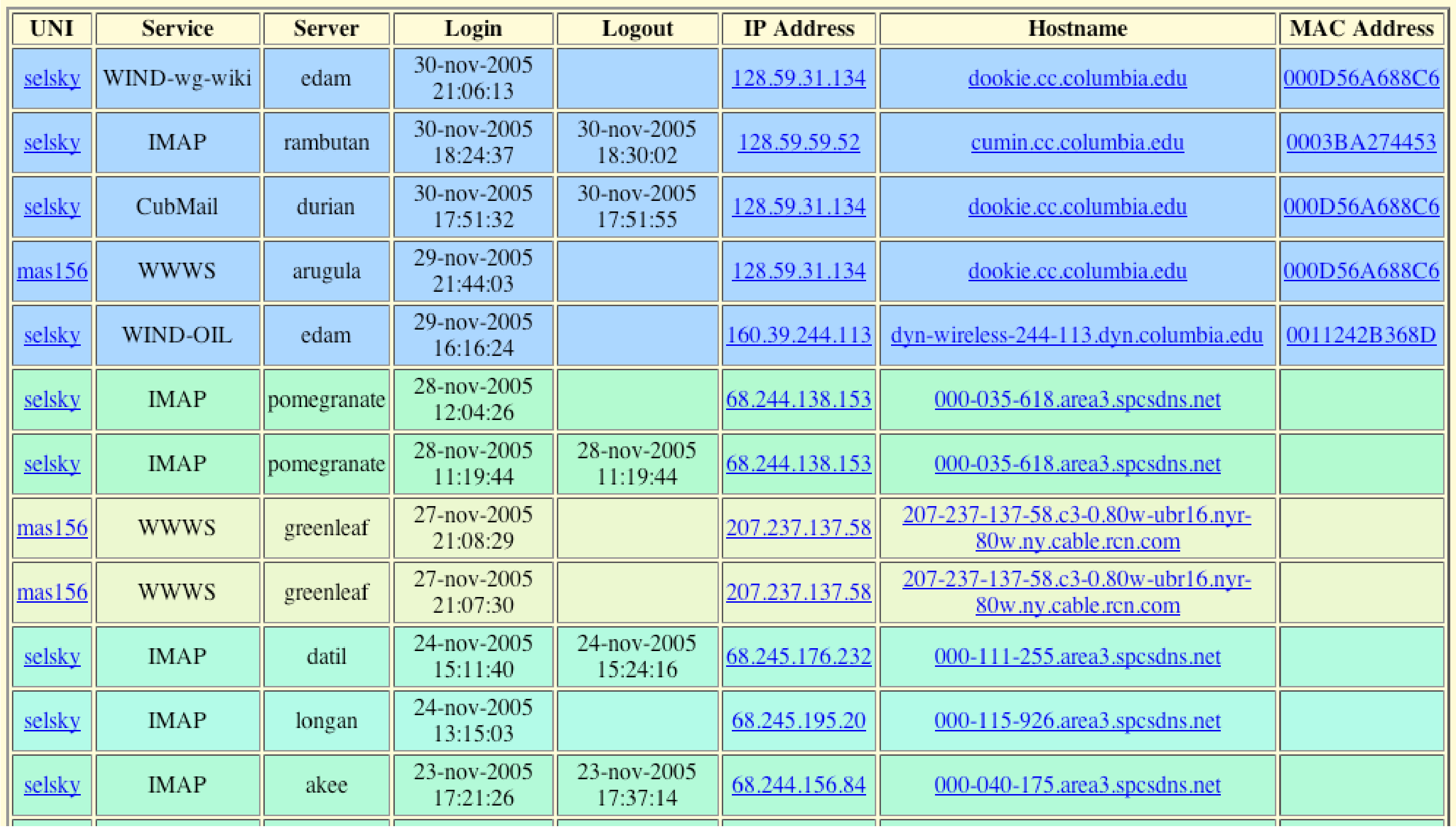


Search User Records

UNI	selsky
IP	
MAC	
Service	
Server	
Start	
End	

Color code:
○ UNI ● IP ○ MAC

GULP – search for user

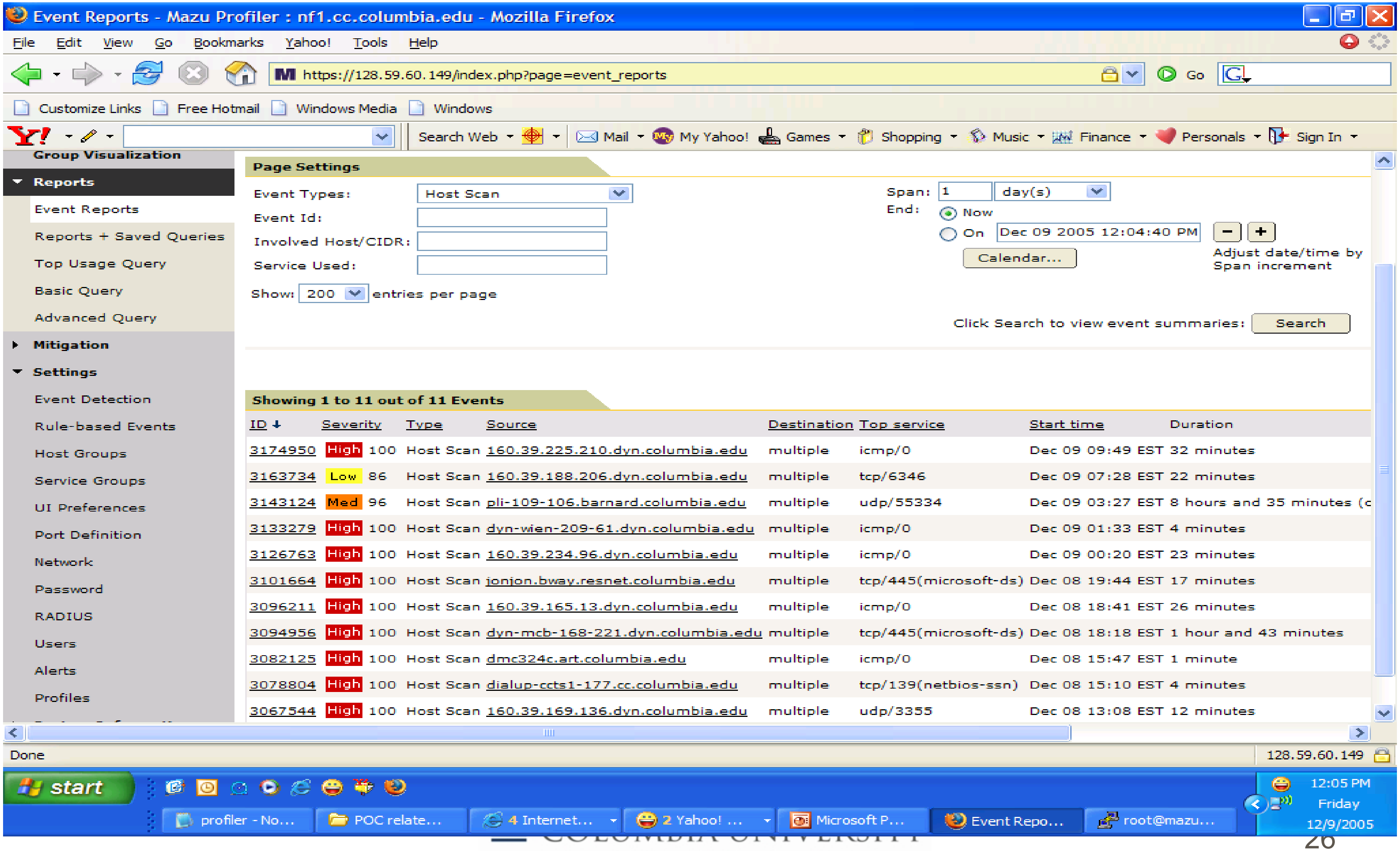


UNI	Service	Server	Login	Logout	IP Address	Hostname	MAC Address
selsky	WIND-wg-wiki	edam	30-nov-2005 21:06:13		128.59.31.134	dookie.cc.columbia.edu	000D56A688C6
selsky	IMAP	rambutan	30-nov-2005 18:24:37	30-nov-2005 18:30:02	128.59.59.52	cumin.cc.columbia.edu	0003BA274453
selsky	CubMail	durian	30-nov-2005 17:51:32	30-nov-2005 17:51:55	128.59.31.134	dookie.cc.columbia.edu	000D56A688C6
mas156	WWWS	arugula	29-nov-2005 21:44:03		128.59.31.134	dookie.cc.columbia.edu	000D56A688C6
selsky	WIND-OIL	edam	29-nov-2005 16:16:24		160.39.244.113	dyn-wireless-244-113.dyn.columbia.edu	0011242B368D
selsky	IMAP	pomegranate	28-nov-2005 12:04:26		68.244.138.153	000-035-618.area3.spcsdns.net	
selsky	IMAP	pomegranate	28-nov-2005 11:19:44	28-nov-2005 11:19:44	68.244.138.153	000-035-618.area3.spcsdns.net	
mas156	WWWS	greenleaf	27-nov-2005 21:08:29		207.237.137.58	207-237-137-58.c3-0.80w-ubr16.nyr-80w.ny.cable.rcn.com	
mas156	WWWS	greenleaf	27-nov-2005 21:07:30		207.237.137.58	207-237-137-58.c3-0.80w-ubr16.nyr-80w.ny.cable.rcn.com	
selsky	IMAP	datil	24-nov-2005 15:11:40	24-nov-2005 15:24:16	68.245.176.232	000-111-255.area3.spcsdns.net	
selsky	IMAP	longan	24-nov-2005 13:15:03		68.245.195.20	000-115-926.area3.spcsdns.net	
selsky	IMAP	akee	23-nov-2005 17:21:26	23-nov-2005 17:37:14	68.244.156.84	000-040-175.area3.spcsdns.net	

PAIRS

- Analyzes Netflow for
  - host/port scanning
  - hitting a darknet
  - connecting to known C&C nodes
- Includes a responsible party database
  - by CIDR and domain
- demo

Event Summary



Page Settings

Event Types: Host Scan

Event Id:

Involved Host/CIDR:

Service Used:

Show: 200 entries per page

Span: 1 day(s)

End: ● Now

○ On Dec 09 2005 12:04:40 PM

Calendar...

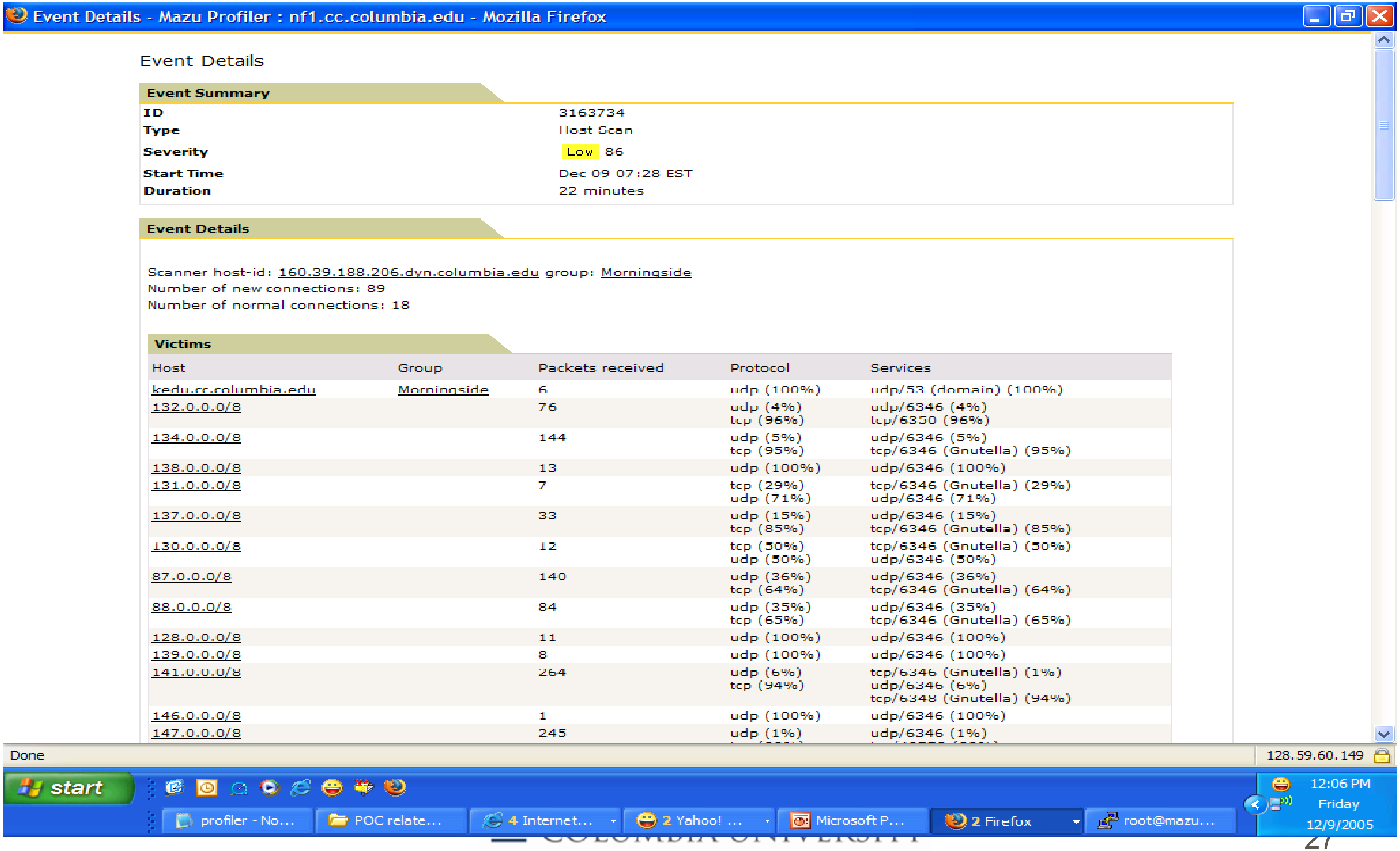
− + Adjust date/time by Span increment

Click Search to view event summaries: Search

Showing 1 to 11 out of 11 Events

ID ↓	Severity		Type	Source	Destination	Top service	Start time	Duration
3174950	High	100	Host Scan	160.39.225.210.dyn.columbia.edu	multiple	icmp/0	Dec 09 09:49 EST	32 minutes
3163734	Low	86	Host Scan	160.39.188.206.dyn.columbia.edu	multiple	tcp/6346	Dec 09 07:28 EST	22 minutes
3143124	Med	96	Host Scan	pli-109-106.barnard.columbia.edu	multiple	udp/55334	Dec 09 03:27 EST	8 hours and 35 minutes (c
3133279	High	100	Host Scan	dyn-wien-209-61.dyn.columbia.edu	multiple	icmp/0	Dec 09 01:33 EST	4 minutes
3126763	High	100	Host Scan	160.39.234.96.dyn.columbia.edu	multiple	icmp/0	Dec 09 00:20 EST	23 minutes
3101664	High	100	Host Scan	jonjon.bway.resnet.columbia.edu	multiple	tcp/445(microsoft-ds)	Dec 08 19:44 EST	17 minutes
3096211	High	100	Host Scan	160.39.165.13.dyn.columbia.edu	multiple	icmp/0	Dec 08 18:41 EST	26 minutes
3094956	High	100	Host Scan	dyn-mcb-168-221.dyn.columbia.edu	multiple	tcp/445(microsoft-ds)	Dec 08 18:18 EST	1 hour and 43 minutes
3082125	High	100	Host Scan	dmc324c.art.columbia.edu	multiple	icmp/0	Dec 08 15:47 EST	1 minute
3078804	High	100	Host Scan	dialup-ccts1-177.cc.columbia.edu	multiple	tcp/139(netbios-ssn)	Dec 08 15:10 EST	4 minutes
3067544	High	100	Host Scan	160.39.169.136.dyn.columbia.edu	multiple	udp/3355	Dec 08 13:08 EST	12 minutes

Host Scan Event



Event Details

Event Summary

ID	3163734
Type	Host Scan
Severity	Low 86
Start Time	Dec 09 07:28 EST
Duration	22 minutes

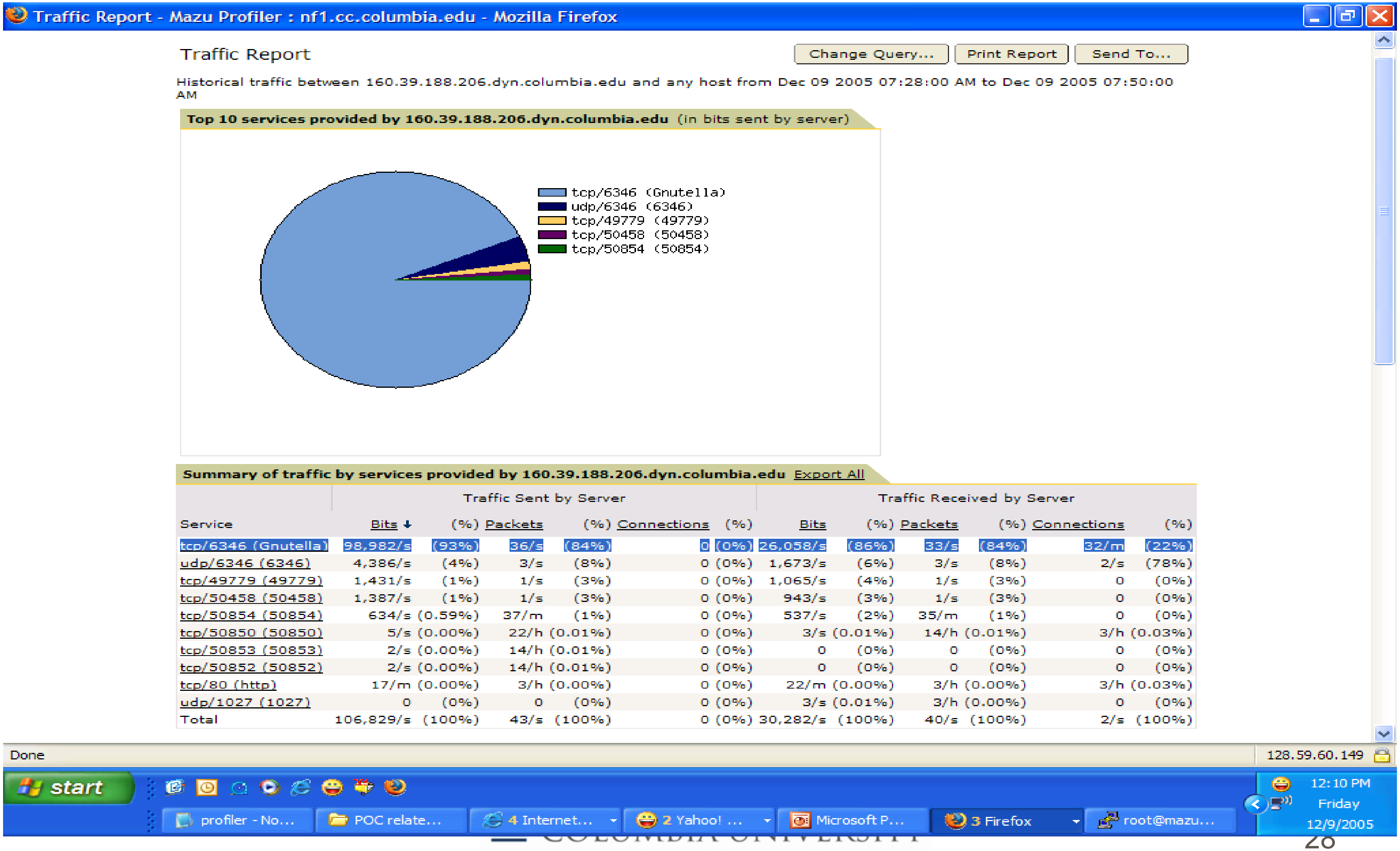
Event Details

Scanner host-id: 160.39.188.206.dyn.columbia.edu group: Morningside
Number of new connections: 89
Number of normal connections: 18

Victims

Host	Group	Packets received	Protocol	Services
kedu.cc.columbia.edu	Morningside	6	udp (100%)	udp/53 (domain) (100%)
132.0.0.0/8		76	udp (4%) tcp (96%)	udp/6346 (4%) tcp/6350 (96%)
134.0.0.0/8		144	udp (5%) tcp (95%)	udp/6346 (5%) tcp/6346 (Gnutella) (95%)
138.0.0.0/8		13	udp (100%)	udp/6346 (100%)
131.0.0.0/8		7	tcp (29%) udp (71%)	tcp/6346 (Gnutella) (29%) udp/6346 (71%)
137.0.0.0/8		33	udp (15%) tcp (85%)	udp/6346 (15%) tcp/6346 (Gnutella) (85%)
130.0.0.0/8		12	tcp (50%) udp (50%)	tcp/6346 (Gnutella) (50%) udp/6346 (50%)
87.0.0.0/8		140	udp (36%) tcp (64%)	udp/6346 (36%) tcp/6346 (Gnutella) (64%)
88.0.0.0/8		84	udp (35%) tcp (65%)	udp/6346 (35%) tcp/6346 (Gnutella) (65%)
128.0.0.0/8		11	udp (100%)	udp/6346 (100%)
139.0.0.0/8		8	udp (100%)	udp/6346 (100%)
141.0.0.0/8		264	udp (6%) tcp (94%)	tcp/6346 (Gnutella) (1%) udp/6346 (6%) tcp/6348 (Gnutella) (94%)
146.0.0.0/8		1	udp (100%)	udp/6346 (100%)
147.0.0.0/8		245	udp (1%)	udp/6346 (1%)

Services Provided



Traffic Report

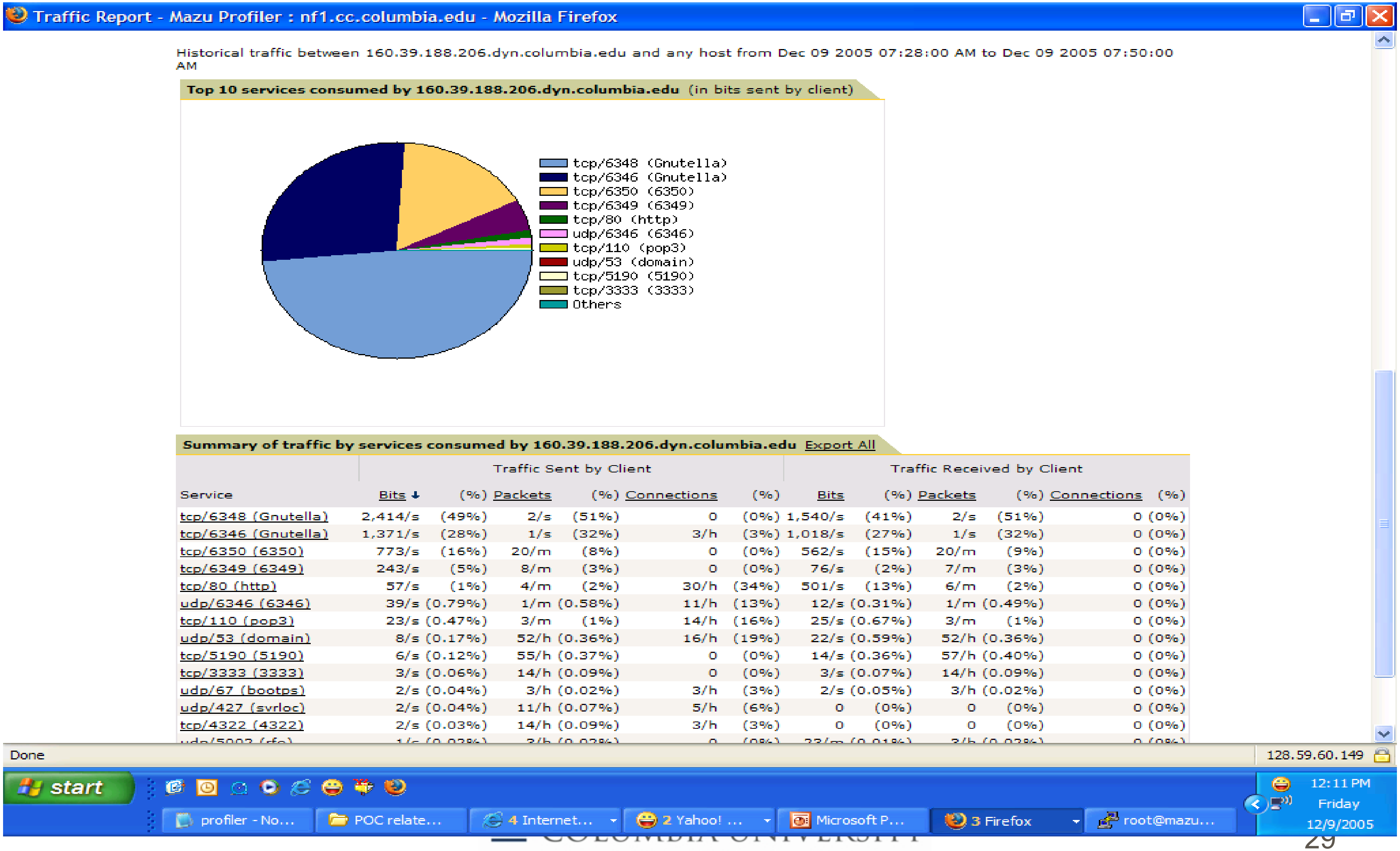
Historical traffic between 160.39.188.206.dyn.columbia.edu and any host from Dec 09 2005 07:28:00 AM to Dec 09 2005 07:50:00 AM

Top 10 services provided by 160.39.188.206.dyn.columbia.edu (in bits sent by server)

Summary of traffic by services provided by 160.39.188.206.dyn.columbia.edu Export All

	Traffic Sent by Server						Traffic Received by Server					
Service	Bits ↓	(%)	Packets	(%)	Connections	(%)	Bits	(%)	Packets	(%)	Connections	(%)
tcp/6346 (Gnutella)	98,982/s	(93%)	36/s	(84%)	0	(0%)	26,058/s	(86%)	33/s	(84%)	32/m	(22%)
udp/6346 (6346)	4,386/s	(4%)	3/s	(8%)	0	(0%)	1,673/s	(6%)	3/s	(8%)	2/s	(78%)
tcp/49779 (49779)	1,431/s	(1%)	1/s	(3%)	0	(0%)	1,065/s	(4%)	1/s	(3%)	0	(0%)
tcp/50458 (50458)	1,387/s	(1%)	1/s	(3%)	0	(0%)	943/s	(3%)	1/s	(3%)	0	(0%)
tcp/50854 (50854)	634/s	(0.59%)	37/m	(1%)	0	(0%)	537/s	(2%)	35/m	(1%)	0	(0%)
tcp/50850 (50850)	5/s	(0.00%)	22/h	(0.01%)	0	(0%)	3/s	(0.01%)	14/h	(0.01%)	3/h	(0.03%)
tcp/50853 (50853)	2/s	(0.00%)	14/h	(0.01%)	0	(0%)	0	(0%)	0	(0%)	0	(0%)
tcp/50852 (50852)	2/s	(0.00%)	14/h	(0.01%)	0	(0%)	0	(0%)	0	(0%)	0	(0%)
tcp/80 (http)	17/m	(0.00%)	3/h	(0.00%)	0	(0%)	22/m	(0.00%)	3/h	(0.00%)	3/h	(0.03%)
udp/1027 (1027)	0	(0%)	0	(0%)	0	(0%)	3/s	(0.01%)	3/h	(0.00%)	0	(0%)
Total	106,829/s	(100%)	43/s	(100%)	0	(0%)	30,282/s	(100%)	40/s	(100%)	2/s	(100%)

Services Consumed



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Historical traffic between 160.39.188.206.dyn.columbia.edu and any host from Dec 09 2005 07:28:00 AM to Dec 09 2005 07:50:00 AM

Top 10 services consumed by 160.39.188.206.dyn.columbia.edu (in bits sent by client)

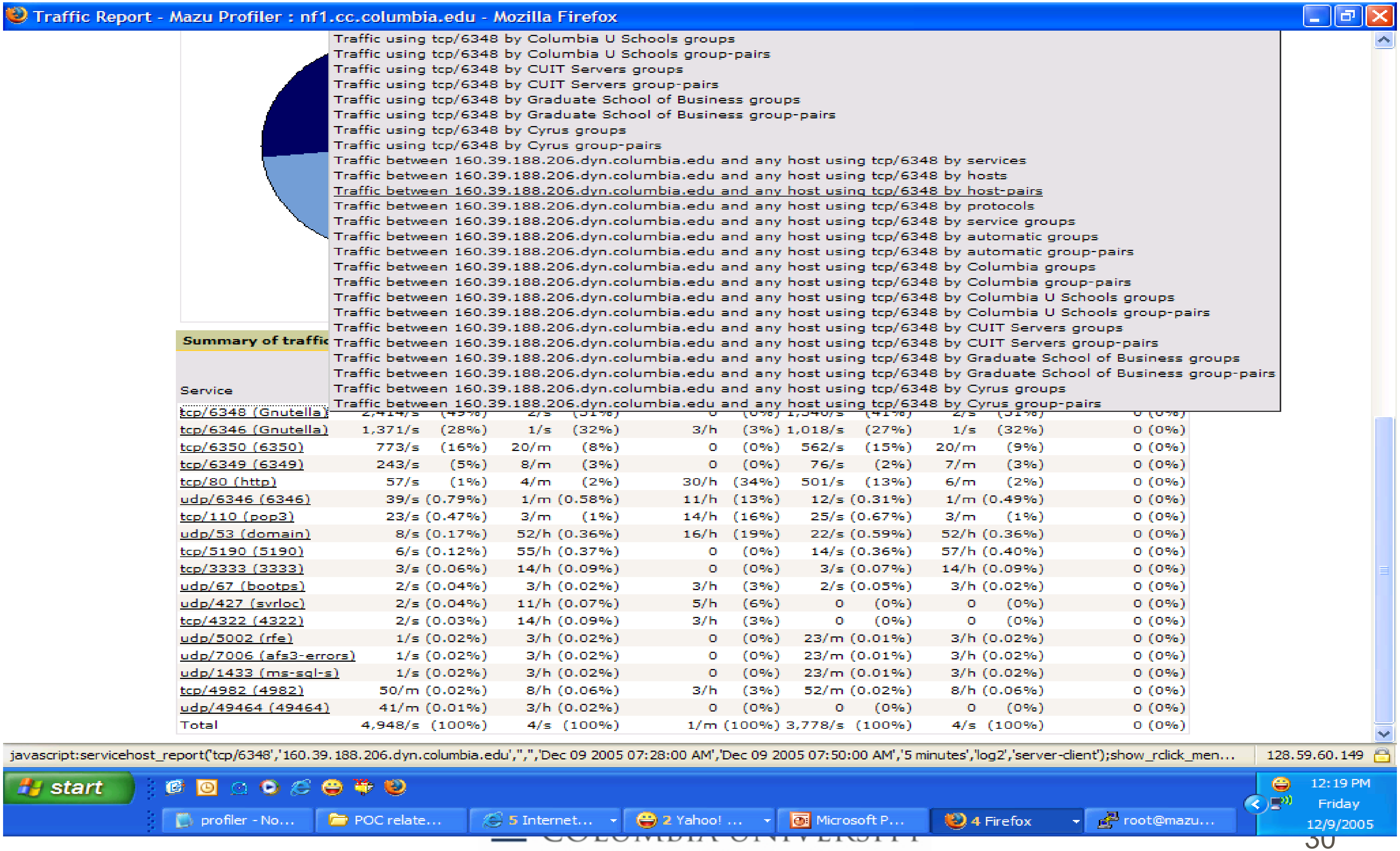
Summary of traffic by services consumed by 160.39.188.206.dyn.columbia.edu Export All

	Traffic Sent by Client						Traffic Received by Client					
Service	Bits ↓	(%)	Packets	(%)	Connections	(%)	Bits	(%)	Packets	(%)	Connections	(%)
tcp/6348 (Gnutella)	2,414/s	(49%)	2/s	(51%)	0	(0%)	1,540/s	(41%)	2/s	(51%)	0	(0%)
tcp/6346 (Gnutella)	1,371/s	(28%)	1/s	(32%)	3/h	(3%)	1,018/s	(27%)	1/s	(32%)	0	(0%)
tcp/6350 (6350)	773/s	(16%)	20/m	(8%)	0	(0%)	562/s	(15%)	20/m	(9%)	0	(0%)
tcp/6349 (6349)	243/s	(5%)	8/m	(3%)	0	(0%)	76/s	(2%)	7/m	(3%)	0	(0%)
tcp/80 (http)	57/s	(1%)	4/m	(2%)	30/h	(34%)	501/s	(13%)	6/m	(2%)	0	(0%)
udp/6346 (6346)	39/s	(0.79%)	1/m	(0.58%)	11/h	(13%)	12/s	(0.31%)	1/m	(0.49%)	0	(0%)
tcp/110 (pop3)	23/s	(0.47%)	3/m	(1%)	14/h	(16%)	25/s	(0.67%)	3/m	(1%)	0	(0%)
udp/53 (domain)	8/s	(0.17%)	52/h	(0.36%)	16/h	(19%)	22/s	(0.59%)	52/h	(0.36%)	0	(0%)
tcp/5190 (5190)	6/s	(0.12%)	55/h	(0.37%)	0	(0%)	14/s	(0.36%)	57/h	(0.40%)	0	(0%)
tcp/3333 (3333)	3/s	(0.06%)	14/h	(0.09%)	0	(0%)	3/s	(0.07%)	14/h	(0.09%)	0	(0%)
udp/67 (bootps)	2/s	(0.04%)	3/h	(0.02%)	3/h	(3%)	2/s	(0.05%)	3/h	(0.02%)	0	(0%)
udp/427 (svrloc)	2/s	(0.04%)	11/h	(0.07%)	5/h	(6%)	0	(0%)	0	(0%)	0	(0%)
tcp/4322 (4322)	2/s	(0.03%)	14/h	(0.09%)	3/h	(3%)	0	(0%)	0	(0%)	0	(0%)
udp/5002 (rfe)	1/s	(0.02%)	3/h	(0.02%)	0	(0%)	23/m	(0.01%)	3/h	(0.02%)	0	(0%)

Done

128.59.60.149

Right-Click (Drill



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

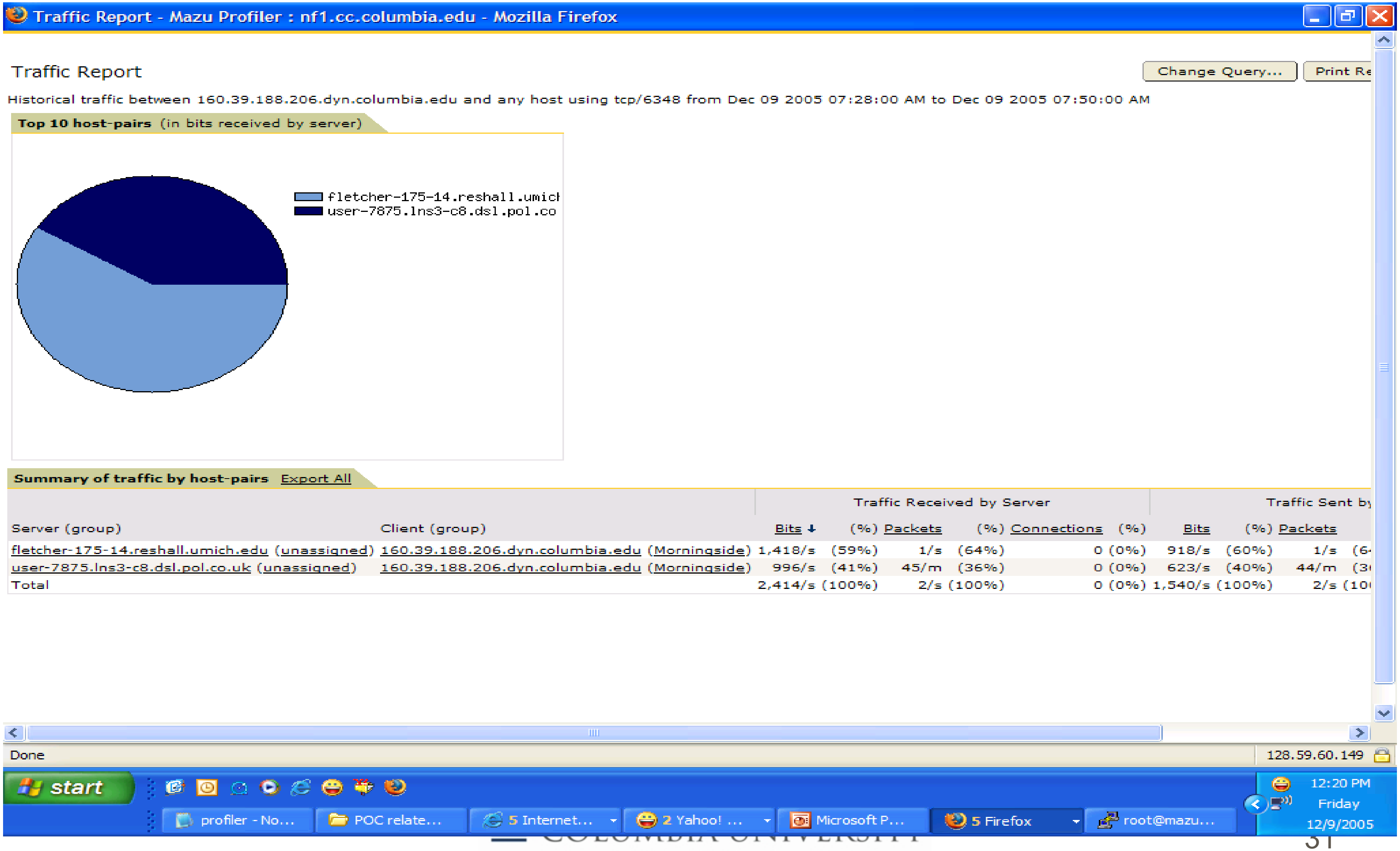
- Traffic using tcp/6348 by Columbia U Schools groups
- Traffic using tcp/6348 by Columbia U Schools group-pairs
- Traffic using tcp/6348 by CUIT Servers groups
- Traffic using tcp/6348 by CUIT Servers group-pairs
- Traffic using tcp/6348 by Graduate School of Business groups
- Traffic using tcp/6348 by Graduate School of Business group-pairs
- Traffic using tcp/6348 by Cyrus groups
- Traffic using tcp/6348 by Cyrus group-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by services
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by hosts
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by host-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by protocols
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by service groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by automatic groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by automatic group-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Columbia groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Columbia group-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Columbia U Schools groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Columbia U Schools group-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by CUIT Servers groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by CUIT Servers group-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Graduate School of Business groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Graduate School of Business group-pairs
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Cyrus groups
- Traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 by Cyrus group-pairs

Summary of traffic

Service						
tcp/6348 (Gnutella)	2,414/s (49%)	2/s (51%)	0 (0%)	1,540/s (41%)	2/s (51%)	0 (0%)
tcp/6346 (Gnutella)	1,371/s (28%)	1/s (32%)	3/h (3%)	1,018/s (27%)	1/s (32%)	0 (0%)
tcp/6350 (6350)	773/s (16%)	20/m (8%)	0 (0%)	562/s (15%)	20/m (9%)	0 (0%)
tcp/6349 (6349)	243/s (5%)	8/m (3%)	0 (0%)	76/s (2%)	7/m (3%)	0 (0%)
tcp/80 (http)	57/s (1%)	4/m (2%)	30/h (34%)	501/s (13%)	6/m (2%)	0 (0%)
udp/6346 (6346)	39/s (0.79%)	1/m (0.58%)	11/h (13%)	12/s (0.31%)	1/m (0.49%)	0 (0%)
tcp/110 (pop3)	23/s (0.47%)	3/m (1%)	14/h (16%)	25/s (0.67%)	3/m (1%)	0 (0%)
udp/53 (domain)	8/s (0.17%)	52/h (0.36%)	16/h (19%)	22/s (0.59%)	52/h (0.36%)	0 (0%)
tcp/5190 (5190)	6/s (0.12%)	55/h (0.37%)	0 (0%)	14/s (0.36%)	57/h (0.40%)	0 (0%)
tcp/3333 (3333)	3/s (0.06%)	14/h (0.09%)	0 (0%)	3/s (0.07%)	14/h (0.09%)	0 (0%)
udp/67 (bootps)	2/s (0.04%)	3/h (0.02%)	3/h (3%)	2/s (0.05%)	3/h (0.02%)	0 (0%)
udp/427 (svrloc)	2/s (0.04%)	11/h (0.07%)	5/h (6%)	0 (0%)	0 (0%)	0 (0%)
tcp/4322 (4322)	2/s (0.03%)	14/h (0.09%)	3/h (3%)	0 (0%)	0 (0%)	0 (0%)
udp/5002 (rfe)	1/s (0.02%)	3/h (0.02%)	0 (0%)	23/m (0.01%)	3/h (0.02%)	0 (0%)
udp/7006 (afs3-errors)	1/s (0.02%)	3/h (0.02%)	0 (0%)	23/m (0.01%)	3/h (0.02%)	0 (0%)
udp/1433 (ms-sql-s)	1/s (0.02%)	3/h (0.02%)	0 (0%)	23/m (0.01%)	3/h (0.02%)	0 (0%)
tcp/4982 (4982)	50/m (0.02%)	8/h (0.06%)	3/h (3%)	52/m (0.02%)	8/h (0.06%)	0 (0%)
udp/49464 (49464)	41/m (0.01%)	3/h (0.02%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Total	4,948/s (100%)	4/s (100%)	1/m (100%)	3,778/s (100%)	4/s (100%)	0 (0%)

javascript:servicehost_report('tcp/6348','160.39.188.206.dyn.columbia.edu','','','Dec 09 2005 07:28:00 AM','Dec 09 2005 07:50:00 AM','5 minutes','log2','server-client');show_rclick_men... 128.59.60.149

Gnutella Peers



Traffic Report

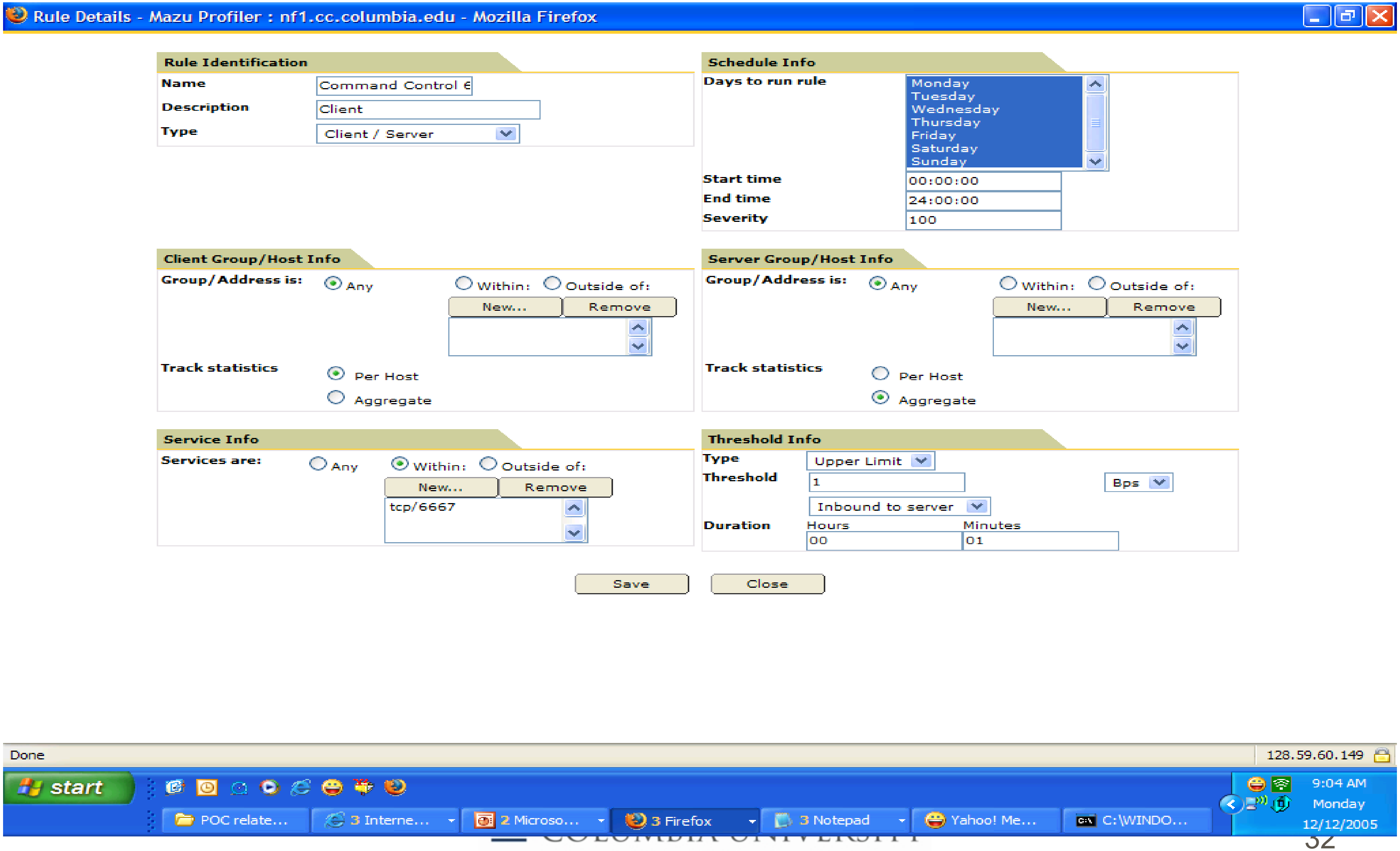
Historical traffic between 160.39.188.206.dyn.columbia.edu and any host using tcp/6348 from Dec 09 2005 07:28:00 AM to Dec 09 2005 07:50:00 AM

Top 10 host-pairs (in bits received by server)

Summary of traffic by host-pairs Export All

		Traffic Received by Server						Traffic Sent by			
Server (group)	Client (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)	Bits	(%)	Packets	
fletcher-175-14.reshall.umich.edu (unassigned)	160.39.188.206.dyn.columbia.edu (Morningside)	1,418/s	(59%)	1/s	(64%)	0	(0%)	918/s	(60%)	1/s	(6
user-7875.lns3-c8.dsl.pol.co.uk (unassigned)	160.39.188.206.dyn.columbia.edu (Morningside)	996/s	(41%)	45/m	(36%)	0	(0%)	623/s	(40%)	44/m	(3
Total		2,414/s	(100%)	2/s	(100%)	0	(0%)	1,540/s	(100%)	2/s	(10

Policy to Detect



Rule Details - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Rule Identification

Name	Command Control €
Description	Client
Type	Client / Server

Schedule Info

Days to run rule	Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Start time	00:00:00
End time	24:00:00
Severity	100

Client Group/Host Info

Group/Address is: ● Any ○ Within: ○ Outside of:

Track statistics: ● Per Host ○ Aggregate

Server Group/Host Info

Group/Address is: ● Any ○ Within: ○ Outside of:

Track statistics: ○ Per Host ● Aggregate

Service Info

Services are: ○ Any ● Within: ○ Outside of:

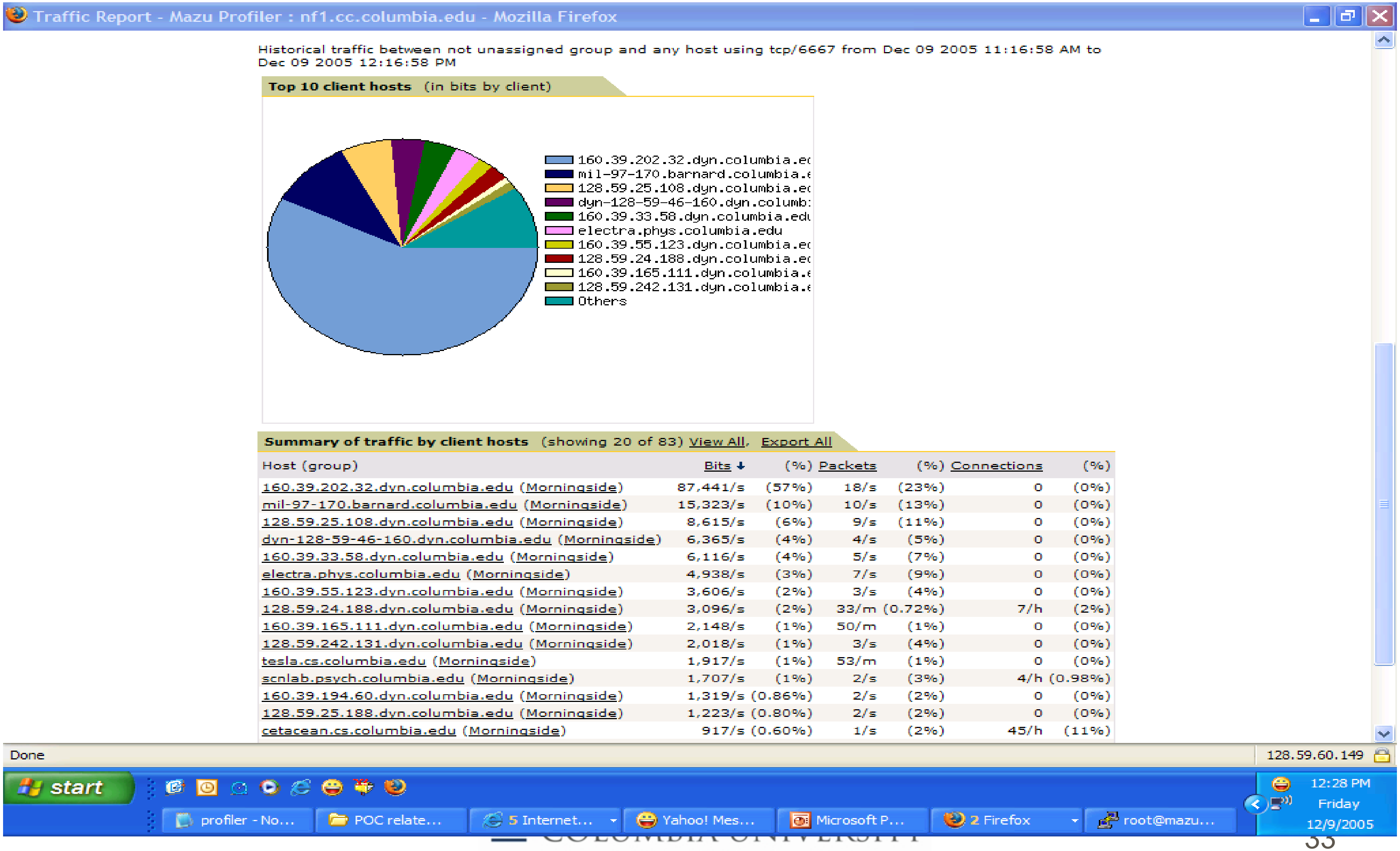
tcp/6667

Threshold Info

Type	Upper Limit
Threshold	1 Bps
	Inbound to server
Duration	Hours 00 Minutes 01

Done 128.59.60.149

Columbia U Owned Hosts


Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox
160.39.202.32.dyn.columbia.ec
mil-97-170.barnard.columbia.e
128.59.25.108.dyn.columbia.ec
dyn-128-59-46-160.dyn.columb:
160.39.33.58.dyn.columbia.edu
electra.phys.columbia.edu
160.39.55.123.dyn.columbia.ec
128.59.24.188.dyn.columbia.ec
160.39.165.111.dyn.columbia.e
128.59.242.131.dyn.columbia.e
Others
Done
128.59.60.149
start
profiler - No...
POC relate...
5 Internet...
Yahoo! Mes...
Microsoft P...
2 Firefox
root@mazu...
12:28 PM
Friday
12/9/2005

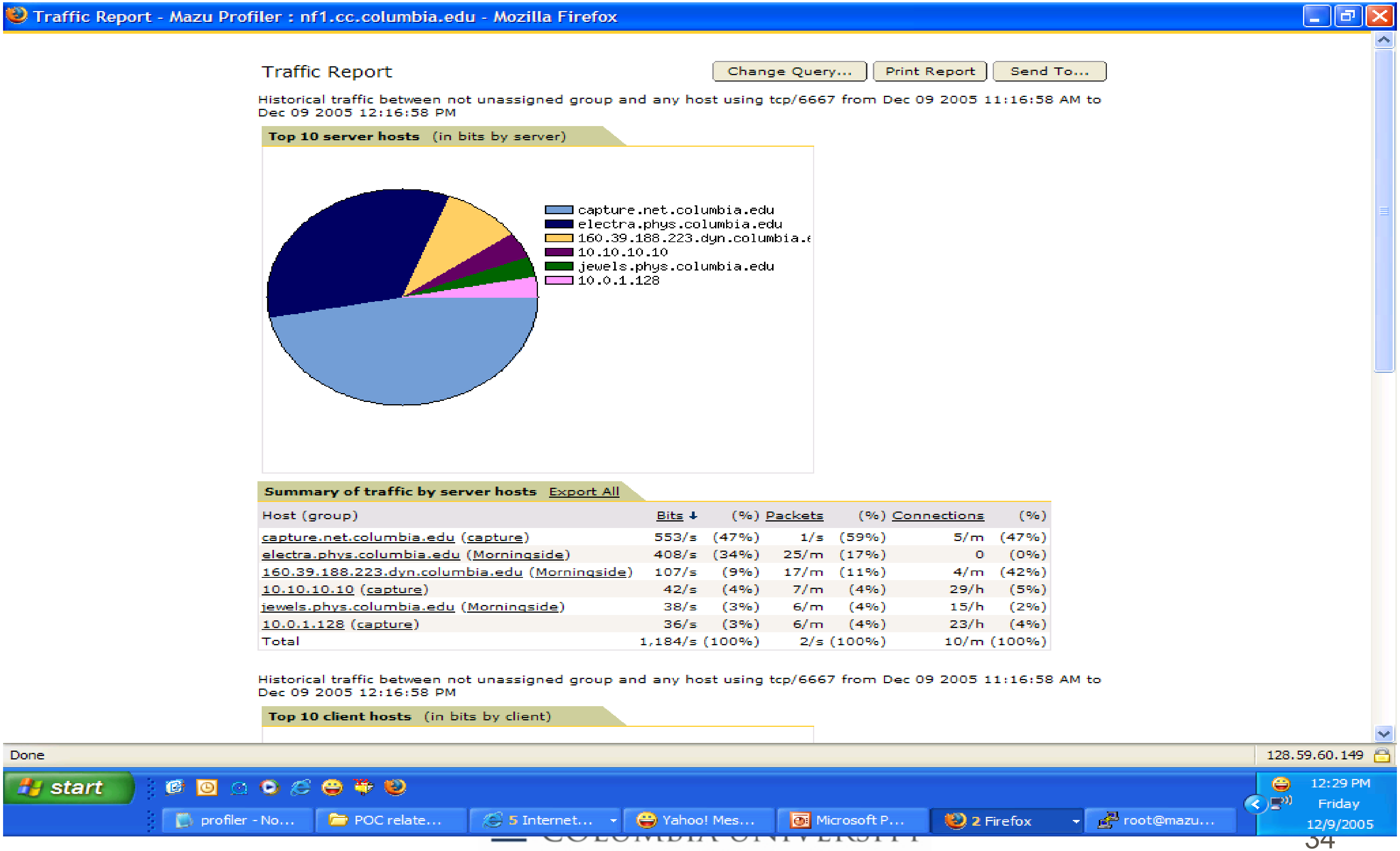
Historical traffic between not unassigned group and any host using tcp/6667 from Dec 09 2005 11:16:58 AM to Dec 09 2005 12:16:58 PM

Top 10 client hosts (in bits by client)

Summary of traffic by client hosts (showing 20 of 83) View All, Export All

Host (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)
160.39.202.32.dyn.columbia.edu (Morningside)	87,441/s	(57%)	18/s	(23%)	0	(0%)
mil-97-170.barnard.columbia.edu (Morningside)	15,323/s	(10%)	10/s	(13%)	0	(0%)
128.59.25.108.dyn.columbia.edu (Morningside)	8,615/s	(6%)	9/s	(11%)	0	(0%)
dyn-128-59-46-160.dyn.columbia.edu (Morningside)	6,365/s	(4%)	4/s	(5%)	0	(0%)
160.39.33.58.dyn.columbia.edu (Morningside)	6,116/s	(4%)	5/s	(7%)	0	(0%)
electra.phys.columbia.edu (Morningside)	4,938/s	(3%)	7/s	(9%)	0	(0%)
160.39.55.123.dyn.columbia.edu (Morningside)	3,606/s	(2%)	3/s	(4%)	0	(0%)
128.59.24.188.dyn.columbia.edu (Morningside)	3,096/s	(2%)	33/m	(0.72%)	7/h	(2%)
160.39.165.111.dyn.columbia.edu (Morningside)	2,148/s	(1%)	50/m	(1%)	0	(0%)
128.59.242.131.dyn.columbia.edu (Morningside)	2,018/s	(1%)	3/s	(4%)	0	(0%)
tesla.cs.columbia.edu (Morningside)	1,917/s	(1%)	53/m	(1%)	0	(0%)
scnlab.psych.columbia.edu (Morningside)	1,707/s	(1%)	2/s	(3%)	4/h	(0.98%)
160.39.194.60.dyn.columbia.edu (Morningside)	1,319/s	(0.86%)	2/s	(2%)	0	(0%)
128.59.25.188.dyn.columbia.edu (Morningside)	1,223/s	(0.80%)	2/s	(2%)	0	(0%)
cetacean.cs.columbia.edu (Morningside)	917/s	(0.60%)	1/s	(2%)	45/h	(11%)

Columbia Owned Hosts



Traffic Report

Historical traffic between not unassigned group and any host using tcp/6667 from Dec 09 2005 11:16:58 AM to Dec 09 2005 12:16:58 PM

Top 10 server hosts (in bits by server)

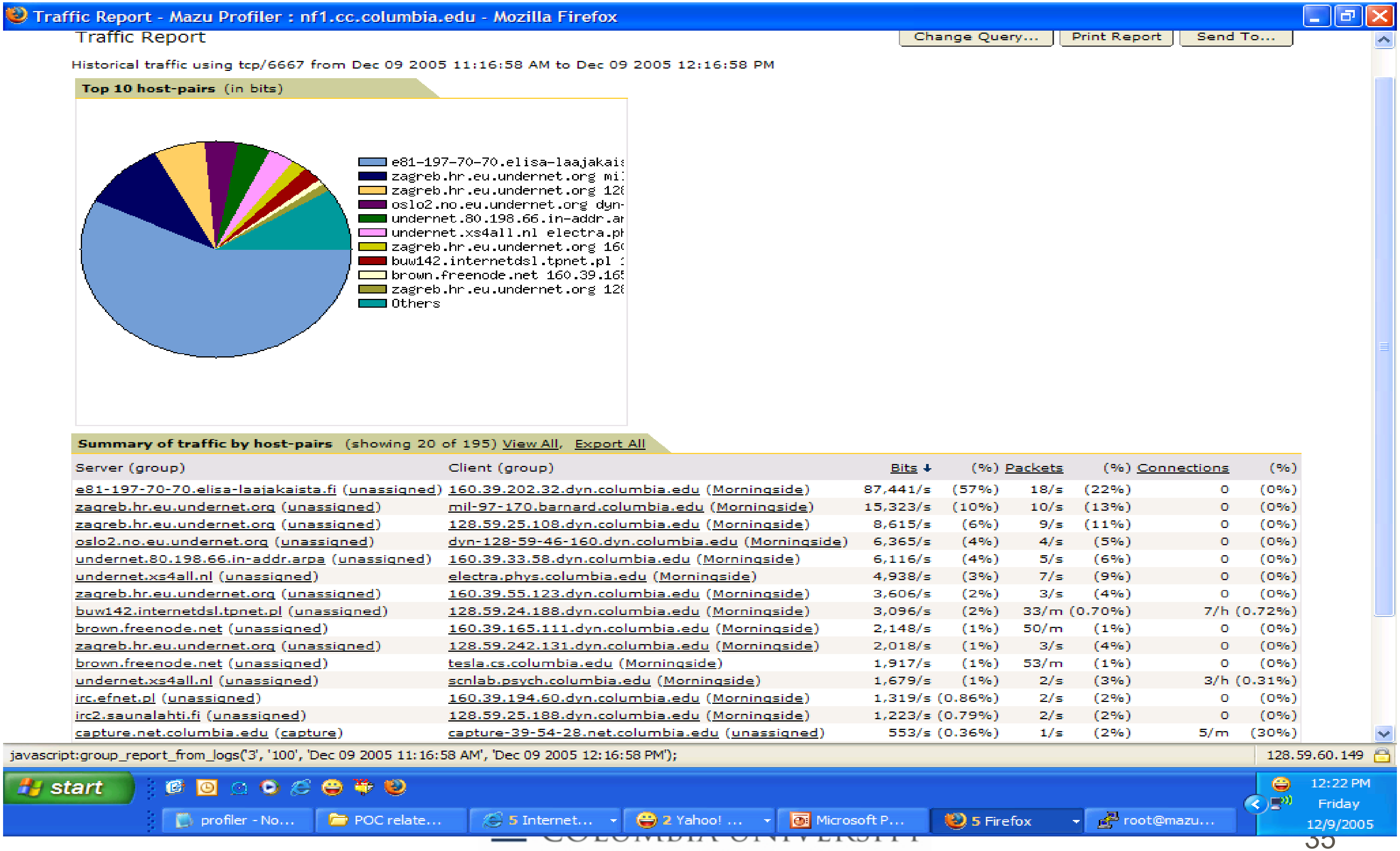
Summary of traffic by server hosts Export All

Host (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)
capture.net.columbia.edu (capture)	553/s	(47%)	1/s	(59%)	5/m	(47%)
electra.phys.columbia.edu (Morningside)	408/s	(34%)	25/m	(17%)	0	(0%)
160.39.188.223.dyn.columbia.edu (Morningside)	107/s	(9%)	17/m	(11%)	4/m	(42%)
10.10.10.10 (capture)	42/s	(4%)	7/m	(4%)	29/h	(5%)
jewels.phys.columbia.edu (Morningside)	38/s	(3%)	6/m	(4%)	15/h	(2%)
10.0.1.128 (capture)	36/s	(3%)	6/m	(4%)	23/h	(4%)
Total	1,184/s	(100%)	2/s	(100%)	10/m	(100%)

Historical traffic between not unassigned group and any host using tcp/6667 from Dec 09 2005 11:16:58 AM to Dec 09 2005 12:16:58 PM

Top 10 client hosts (in bits by client)

Who is


Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox
Change Query...
Print Report
Send To...
e81-197-70-70.elisa-laajakais
zagreb.hr.eu.undernet.org mil
zagreb.hr.eu.undernet.org 128
oslo2.no.eu.undernet.org dyn-
undernet.80.198.66.in-addr.ar
undernet.xs4all.nl electra.ph
zagreb.hr.eu.undernet.org 160
buw142.internetdsl.tpnet.pl 1
brown.freenode.net 160.39.165
zagreb.hr.eu.undernet.org 128
Others
start
profiler - No...
POC relate...
5 Internet...
2 Yahoo! ...
Microsoft P...
5 Firefox
root@mazu...
12:22 PM
Friday
12/9/2005

Traffic Report

Historical traffic using tcp/6667 from Dec 09 2005 11:16:58 AM to Dec 09 2005 12:16:58 PM

Top 10 host-pairs (in bits)

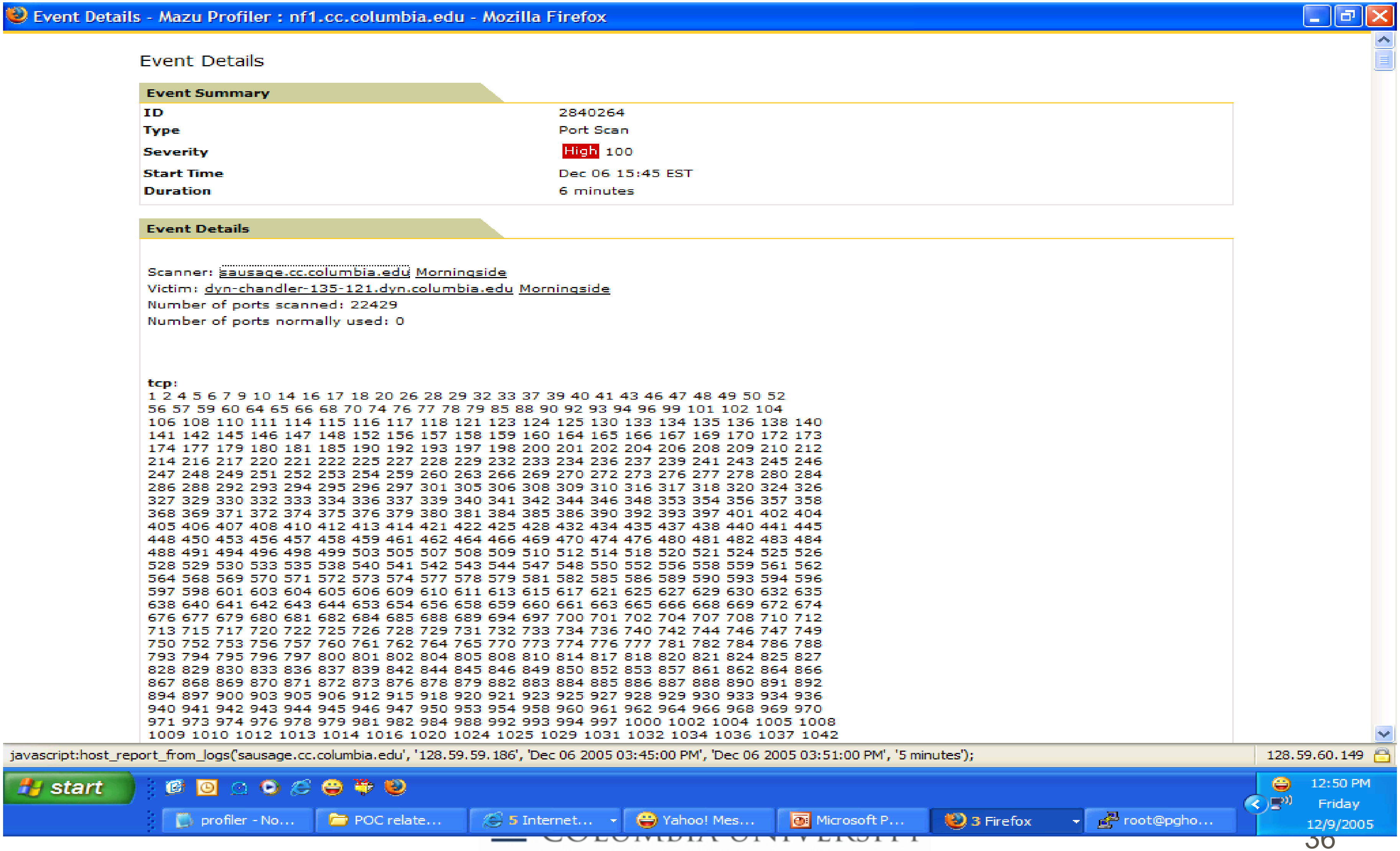
Summary of traffic by host-pairs (showing 20 of 195) View All, Export All

Server (group)	Client (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)
e81-197-70-70.elisa-laajakaista.fi (unassigned)	160.39.202.32.dyn.columbia.edu (Morningside)	87,441/s	(57%)	18/s	(22%)	0	(0%)
zagreb.hr.eu.undernet.org (unassigned)	mil-97-170.barnard.columbia.edu (Morningside)	15,323/s	(10%)	10/s	(13%)	0	(0%)
zagreb.hr.eu.undernet.org (unassigned)	128.59.25.108.dyn.columbia.edu (Morningside)	8,615/s	(6%)	9/s	(11%)	0	(0%)
oslo2.no.eu.undernet.org (unassigned)	dyn-128-59-46-160.dyn.columbia.edu (Morningside)	6,365/s	(4%)	4/s	(5%)	0	(0%)
undernet.80.198.66.in-addr.arpa (unassigned)	160.39.33.58.dyn.columbia.edu (Morningside)	6,116/s	(4%)	5/s	(6%)	0	(0%)
undernet.xs4all.nl (unassigned)	electra.phys.columbia.edu (Morningside)	4,938/s	(3%)	7/s	(9%)	0	(0%)
zagreb.hr.eu.undernet.org (unassigned)	160.39.55.123.dyn.columbia.edu (Morningside)	3,606/s	(2%)	3/s	(4%)	0	(0%)
buw142.internetdsl.tpnet.pl (unassigned)	128.59.24.188.dyn.columbia.edu (Morningside)	3,096/s	(2%)	33/m	(0.70%)	7/h	(0.72%)
brown.freenode.net (unassigned)	160.39.165.111.dyn.columbia.edu (Morningside)	2,148/s	(1%)	50/m	(1%)	0	(0%)
zagreb.hr.eu.undernet.org (unassigned)	128.59.242.131.dyn.columbia.edu (Morningside)	2,018/s	(1%)	3/s	(4%)	0	(0%)
brown.freenode.net (unassigned)	tesla.cs.columbia.edu (Morningside)	1,917/s	(1%)	53/m	(1%)	0	(0%)
undernet.xs4all.nl (unassigned)	scnlab.psych.columbia.edu (Morningside)	1,679/s	(1%)	2/s	(3%)	3/h	(0.31%)
irc.efnet.pl (unassigned)	160.39.194.60.dyn.columbia.edu (Morningside)	1,319/s	(0.86%)	2/s	(2%)	0	(0%)
irc2.saunalahti.fi (unassigned)	128.59.25.188.dyn.columbia.edu (Morningside)	1,223/s	(0.79%)	2/s	(2%)	0	(0%)
capture.net.columbia.edu (capture)	capture-39-54-28.net.columbia.edu (unassigned)	553/s	(0.36%)	1/s	(2%)	5/m	(30%)

javascript:group_report_from_logs('3', '100', 'Dec 09 2005 11:16:58 AM', 'Dec 09 2005 12:16:58 PM');

128.59.60.149

Port Scan Event


Event Details - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Event Details

Event Summary

ID	2840264
Type	Port Scan
Severity	High 100
Start Time	Dec 06 15:45 EST
Duration	6 minutes

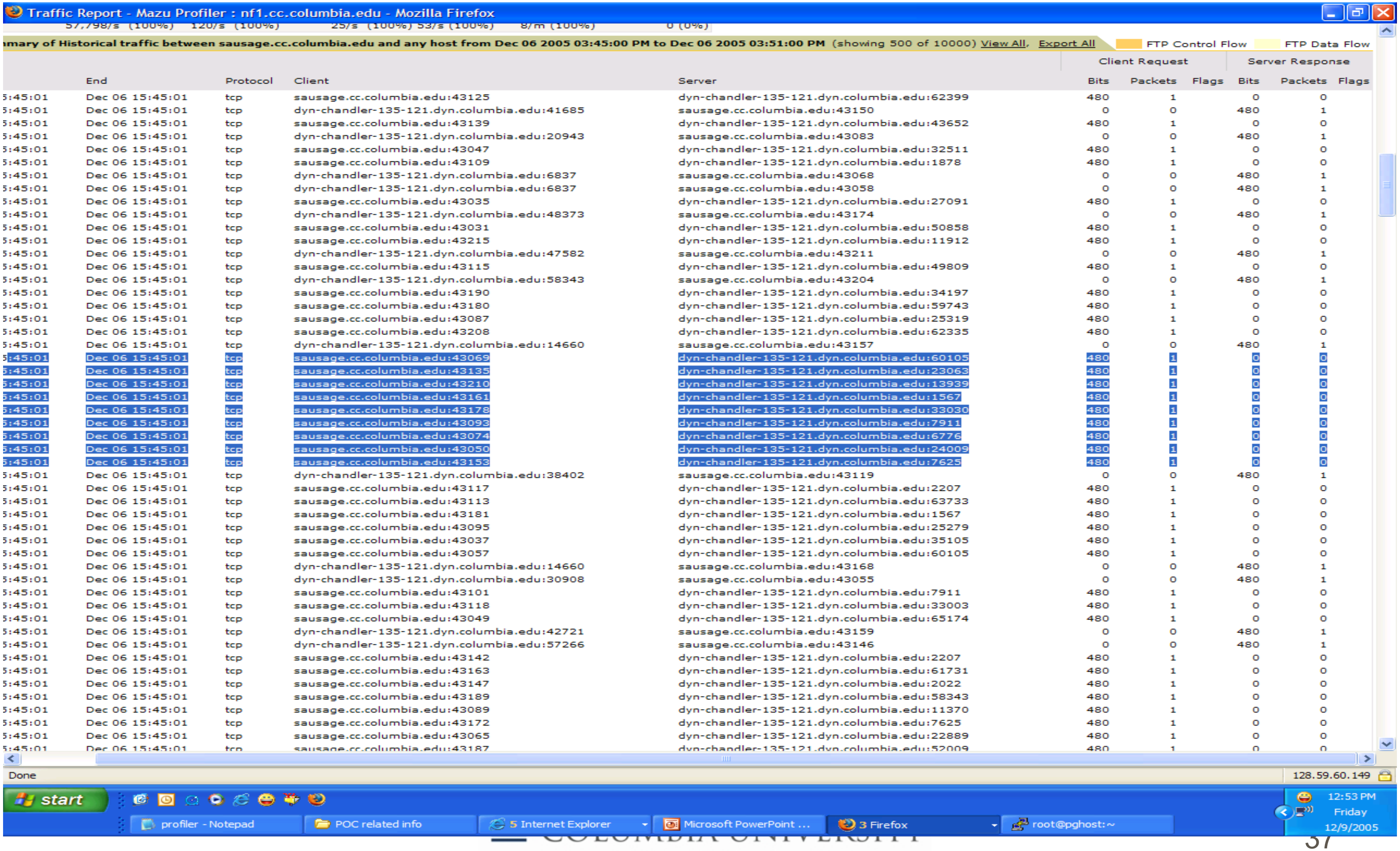
Event Details

```
Scanner: sausage.cc.columbia.edu Morningside
Victim: dyn-chandler-135-121.dyn.columbia.edu Morningside
Number of ports scanned: 22429
Number of ports normally used: 0


tcp:
1 2 4 5 6 7 9 10 14 16 17 18 20 26 28 29 32 33 37 39 40 41 43 46 47 48 49 50 52
56 57 59 60 64 65 66 68 70 74 76 77 78 79 85 88 90 92 93 94 96 99 101 102 104
106 108 110 111 114 115 116 117 118 121 123 124 125 130 133 134 135 136 138 140
141 142 145 146 147 148 152 156 157 158 159 160 164 165 166 167 169 170 172 173
174 177 179 180 181 185 190 192 193 197 198 200 201 202 204 206 208 209 210 212
214 216 217 220 221 222 225 227 228 229 232 233 234 236 237 239 241 243 245 246
247 248 249 251 252 253 254 259 260 263 266 269 270 272 273 276 277 278 280 284
286 288 292 293 294 295 296 297 301 305 306 308 309 310 316 317 318 320 324 326
327 329 330 332 333 334 336 337 339 340 341 342 344 346 348 353 354 356 357 358
368 369 371 372 374 375 376 379 380 381 384 385 386 390 392 393 397 401 402 404
405 406 407 408 410 412 413 414 421 422 425 428 432 434 435 437 438 440 441 445
448 450 453 456 457 458 459 461 462 464 466 469 470 474 476 480 481 482 483 484
488 491 494 496 498 499 503 505 507 508 509 510 512 514 518 520 521 524 525 526
528 529 530 533 535 538 540 541 542 543 544 547 548 550 552 556 558 559 561 562
564 568 569 570 571 572 573 574 577 578 579 581 582 585 586 589 590 593 594 596
597 598 601 603 604 605 606 609 610 611 613 615 617 621 625 627 629 630 632 635
638 640 641 642 643 644 653 654 656 658 659 660 661 663 665 666 668 669 672 674
676 677 679 680 681 682 684 685 688 689 694 697 700 701 702 704 707 708 710 712
713 715 717 720 722 725 726 728 729 731 732 733 734 736 740 742 744 746 747 749
750 752 753 756 757 760 761 762 764 765 770 773 774 776 777 781 782 784 786 788
793 794 795 796 797 800 801 802 804 805 808 810 814 817 818 820 821 824 825 827
828 829 830 833 836 837 839 842 844 845 846 849 850 852 853 857 861 862 864 866
867 868 869 870 871 872 873 876 878 879 882 883 884 885 886 887 888 890 891 892
894 897 900 903 905 906 912 915 918 920 921 923 925 927 928 929 930 933 934 936
940 941 942 943 944 945 946 947 950 953 954 958 960 961 962 964 966 968 969 970
971 973 974 976 978 979 981 982 984 988 992 993 994 997 1000 1002 1004 1005 1008
1009 1010 1012 1013 1014 1016 1020 1024 1025 1029 1031 1032 1034 1036 1037 1042
```

```
javascript:host_report_from_logs('sausage.cc.columbia.edu', '128.59.59.186', 'Dec 06 2005 03:45:00 PM', 'Dec 06 2005 03:51:00 PM', '5 minutes');
```

Detailed



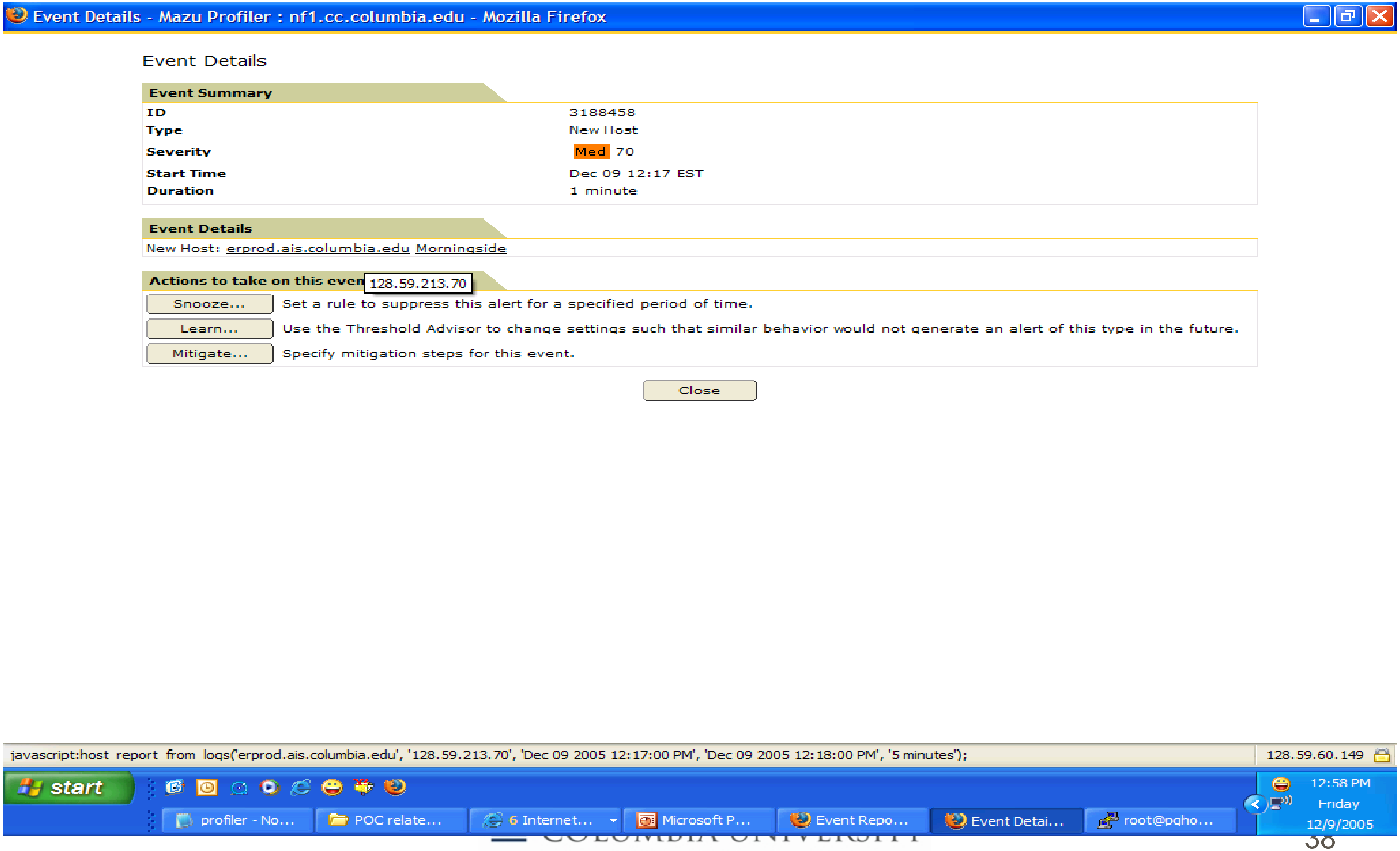
57,798/s (100%) 120/s (100%) 25/s (100%) 53/s (100%) 8/m (100%) 0 (0%)

mary of Historical traffic between sausage.cc.columbia.edu and any host from Dec 06 2005 03:45:00 PM to Dec 06 2005 03:51:00 PM (showing 500 of 10000) View All, Export All

FTP Control Flow FTP Data Flow

					Client Request			Server Response		
	End	Protocol	Client	Server	Bits	Packets	Flags	Bits	Packets	Flags
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43125	dyn-chandler-135-121.dyn.columbia.edu:62399	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:41685	sausage.cc.columbia.edu:43150	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43139	dyn-chandler-135-121.dyn.columbia.edu:43652	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:20943	sausage.cc.columbia.edu:43083	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43047	dyn-chandler-135-121.dyn.columbia.edu:32511	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43109	dyn-chandler-135-121.dyn.columbia.edu:1878	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:6837	sausage.cc.columbia.edu:43068	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:6837	sausage.cc.columbia.edu:43058	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43035	dyn-chandler-135-121.dyn.columbia.edu:27091	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:48373	sausage.cc.columbia.edu:43174	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43031	dyn-chandler-135-121.dyn.columbia.edu:50858	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43215	dyn-chandler-135-121.dyn.columbia.edu:11912	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:47582	sausage.cc.columbia.edu:43211	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43115	dyn-chandler-135-121.dyn.columbia.edu:49809	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:58343	sausage.cc.columbia.edu:43204	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43190	dyn-chandler-135-121.dyn.columbia.edu:34197	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43180	dyn-chandler-135-121.dyn.columbia.edu:59743	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43087	dyn-chandler-135-121.dyn.columbia.edu:25319	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43208	dyn-chandler-135-121.dyn.columbia.edu:62335	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:14660	sausage.cc.columbia.edu:43157	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43069	dyn-chandler-135-121.dyn.columbia.edu:60105	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43135	dyn-chandler-135-121.dyn.columbia.edu:23063	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43210	dyn-chandler-135-121.dyn.columbia.edu:13939	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43161	dyn-chandler-135-121.dyn.columbia.edu:1567	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43178	dyn-chandler-135-121.dyn.columbia.edu:33030	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43093	dyn-chandler-135-121.dyn.columbia.edu:7911	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43074	dyn-chandler-135-121.dyn.columbia.edu:6776	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43050	dyn-chandler-135-121.dyn.columbia.edu:24009	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43153	dyn-chandler-135-121.dyn.columbia.edu:7625	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:38402	sausage.cc.columbia.edu:43119	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43117	dyn-chandler-135-121.dyn.columbia.edu:2207	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43113	dyn-chandler-135-121.dyn.columbia.edu:63733	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43181	dyn-chandler-135-121.dyn.columbia.edu:1567	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43095	dyn-chandler-135-121.dyn.columbia.edu:25279	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43037	dyn-chandler-135-121.dyn.columbia.edu:35105	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43057	dyn-chandler-135-121.dyn.columbia.edu:60105	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:14660	sausage.cc.columbia.edu:43168	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:30908	sausage.cc.columbia.edu:43055	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43101	dyn-chandler-135-121.dyn.columbia.edu:7911	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43118	dyn-chandler-135-121.dyn.columbia.edu:33003	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43049	dyn-chandler-135-121.dyn.columbia.edu:65174	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:42721	sausage.cc.columbia.edu:43159	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	dyn-chandler-135-121.dyn.columbia.edu:57266	sausage.cc.columbia.edu:43146	0	0		480	1	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43142	dyn-chandler-135-121.dyn.columbia.edu:2207	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43163	dyn-chandler-135-121.dyn.columbia.edu:61731	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43147	dyn-chandler-135-121.dyn.columbia.edu:2022	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43189	dyn-chandler-135-121.dyn.columbia.edu:58343	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43089	dyn-chandler-135-121.dyn.columbia.edu:11370	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43172	dyn-chandler-135-121.dyn.columbia.edu:7625	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43065	dyn-chandler-135-121.dyn.columbia.edu:22889	480	1		0	0	
5:45:01	Dec 06 15:45:01	tcp	sausage.cc.columbia.edu:43187	dyn-chandler-135-121.dyn.columbia.edu:52009	480	1		0	0	

New Host Event –



Event Details - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Event Details

Event Summary

ID	3188458
Type	New Host
Severity	Med 70
Start Time	Dec 09 12:17 EST
Duration	1 minute

Event Details

New Host: erprod.ais.columbia.edu Morningside

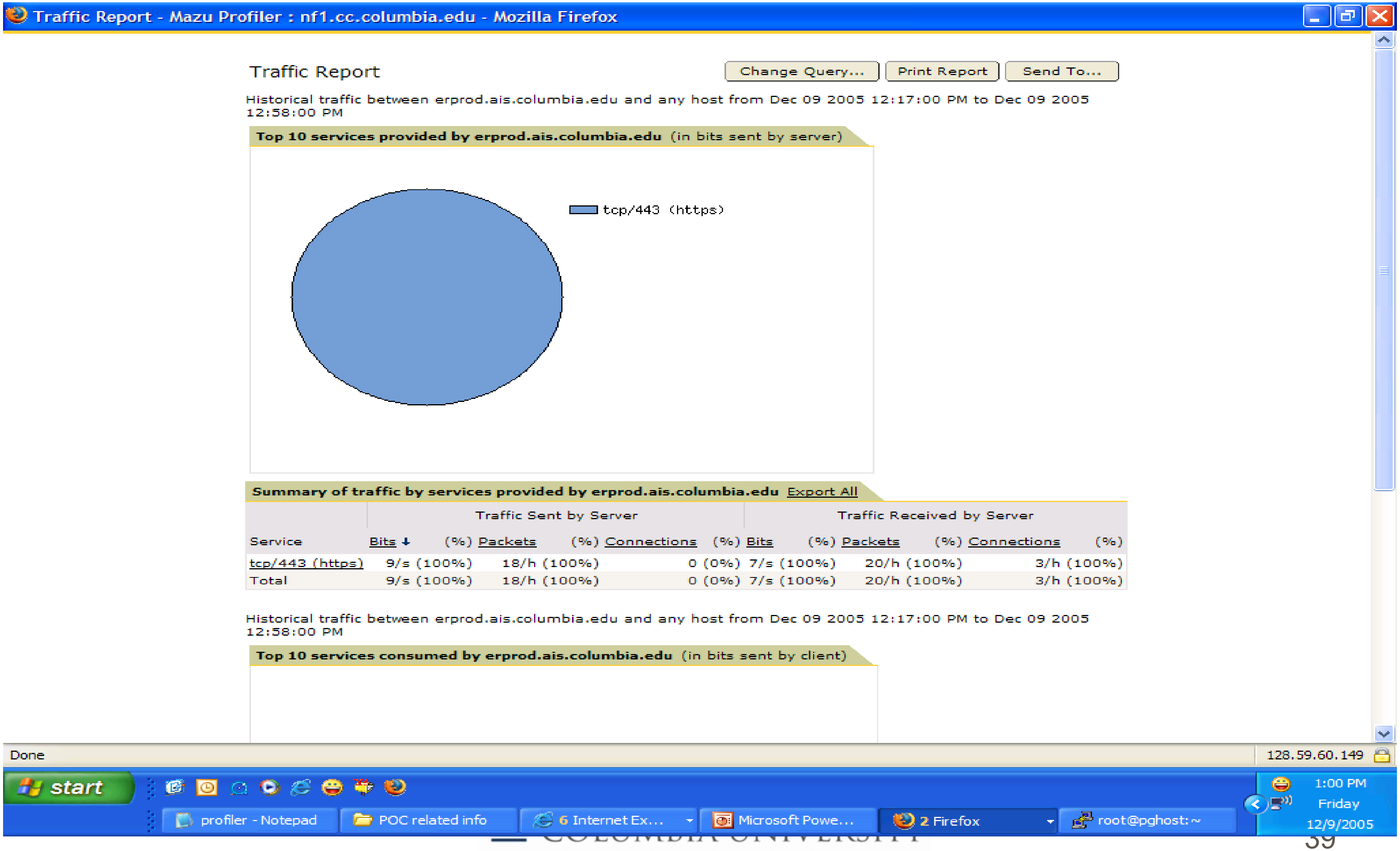
Actions to take on this even 128.59.213.70

Snooze...	Set a rule to suppress this alert for a specified period of time.
Learn...	Use the Threshold Advisor to change settings such that similar behavior would not generate an alert of this type in the future.
Mitigate...	Specify mitigation steps for this event.

Close

javascript:host_report_from_logs('erprod.ais.columbia.edu', '128.59.213.70', 'Dec 09 2005 12:17:00 PM', 'Dec 09 2005 12:18:00 PM', '5 minutes'); 128.59.60.149

Services Provided by



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Traffic Report

Historical traffic between erprod.ais.columbia.edu and any host from Dec 09 2005 12:17:00 PM to Dec 09 2005 12:58:00 PM

Top 10 services provided by erprod.ais.columbia.edu (in bits sent by server)

Summary of traffic by services provided by erprod.ais.columbia.edu Export All

	Traffic Sent by Server			Traffic Received by Server		
Service	Bits ↓ (%)	Packets (%)	Connections (%)	Bits (%)	Packets (%)	Connections (%)
tcp/443 (https)	9/s (100%)	18/h (100%)	0 (0%)	7/s (100%)	20/h (100%)	3/h (100%)
Total	9/s (100%)	18/h (100%)	0 (0%)	7/s (100%)	20/h (100%)	3/h (100%)

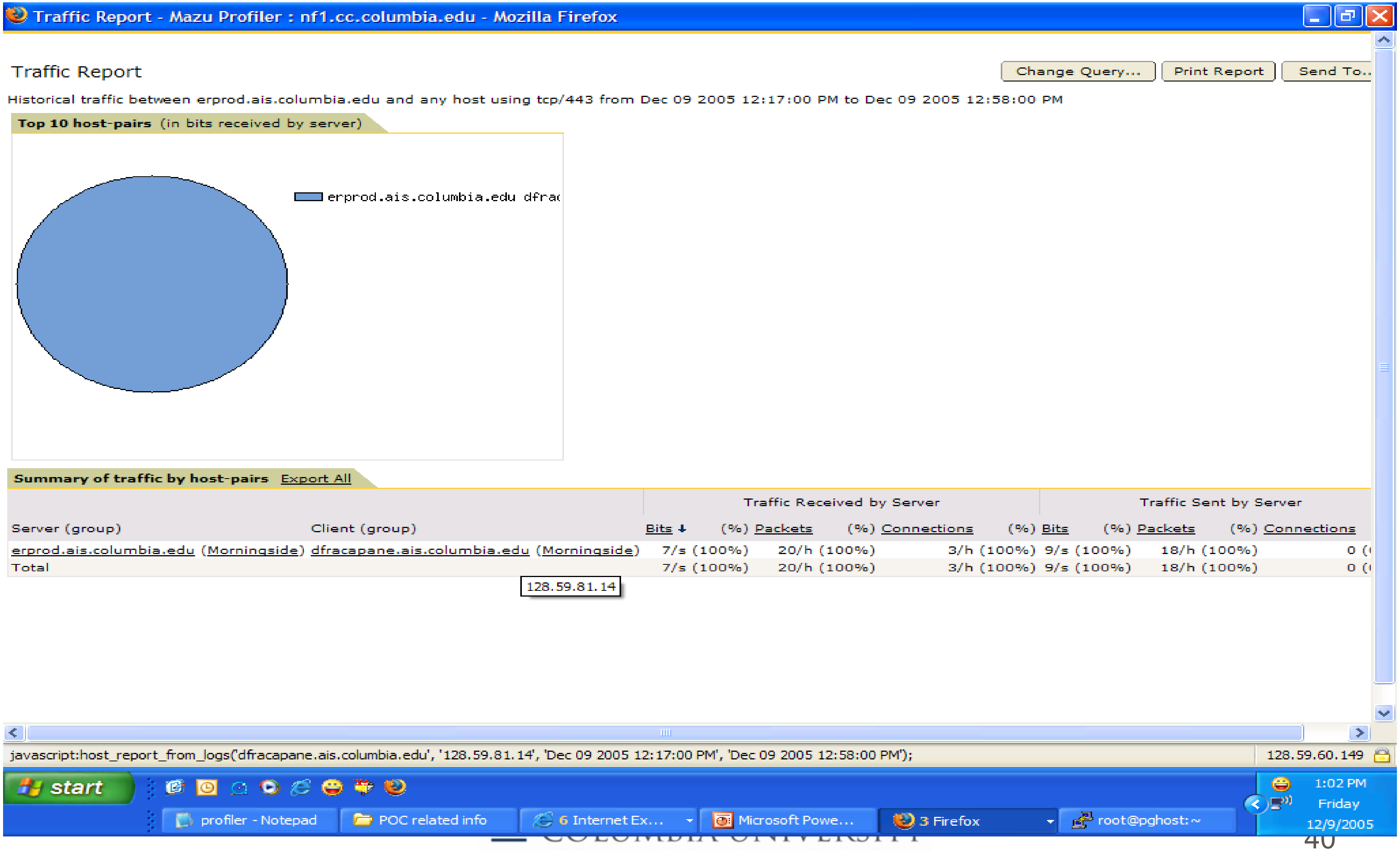
Historical traffic between erprod.ais.columbia.edu and any host from Dec 09 2005 12:17:00 PM to Dec 09 2005 12:58:00 PM

Top 10 services consumed by erprod.ais.columbia.edu (in bits sent by client)

Done

128.59.60.149

To Whom?



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Traffic Report

Historical traffic between erprod.ais.columbia.edu and any host using tcp/443 from Dec 09 2005 12:17:00 PM to Dec 09 2005 12:58:00 PM

Top 10 host-pairs (in bits received by server)

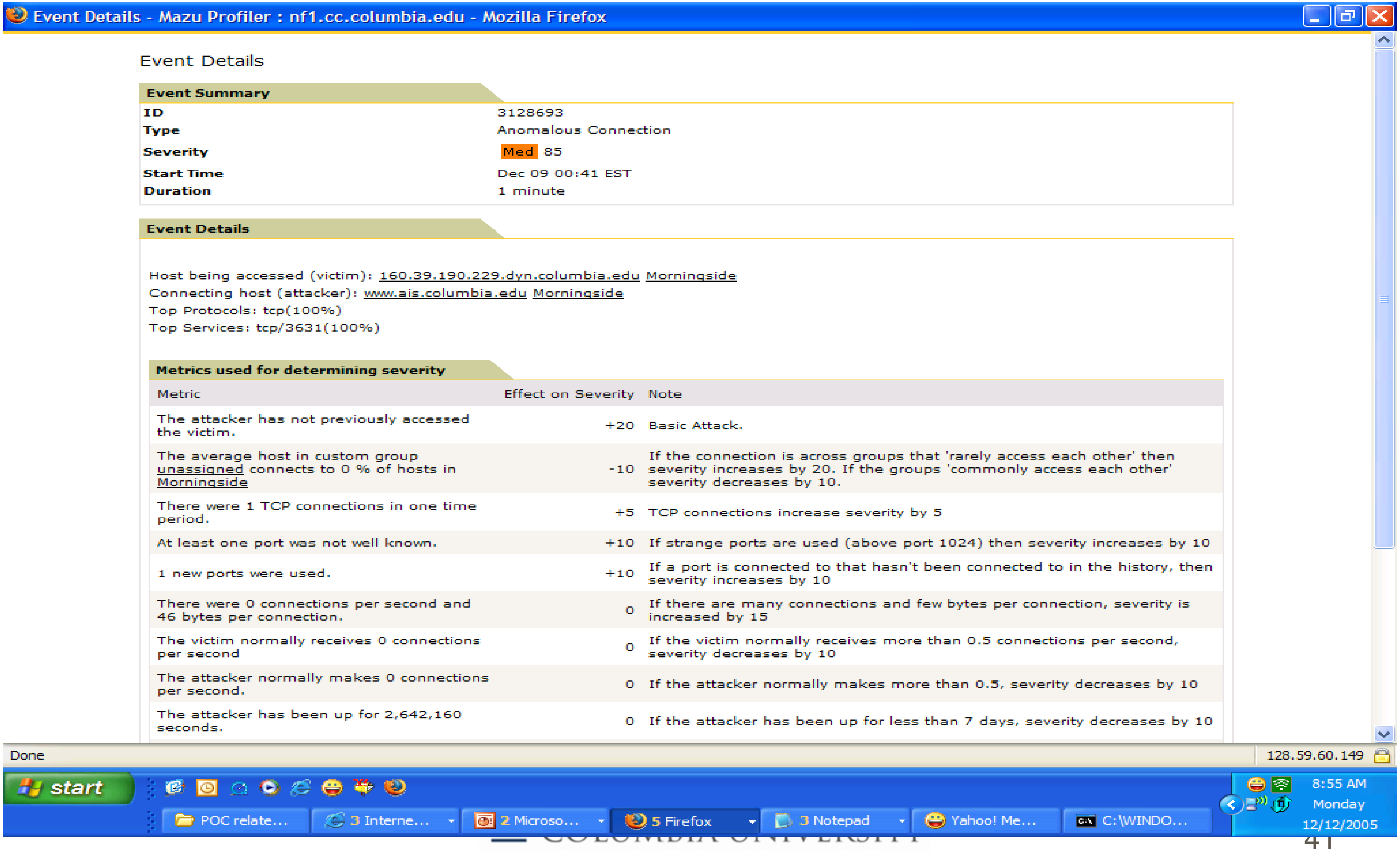
Summary of traffic by host-pairs Export All

		Traffic Received by Server			Traffic Sent by Server		
Server (group)	Client (group)	Bits ↓ (%)	Packets (%)	Connections (%)	Bits (%)	Packets (%)	Connections
erprod.ais.columbia.edu (Morningside)	dfracapane.ais.columbia.edu (Morningside)	7/s (100%)	20/h (100%)	3/h (100%)	9/s (100%)	18/h (100%)	0 (
Total		7/s (100%)	20/h (100%)	3/h (100%)	9/s (100%)	18/h (100%)	0 (

128.59.81.14

javascript:host_report_from_logs('dfracapane.ais.columbia.edu', '128.59.81.14', 'Dec 09 2005 12:17:00 PM', 'Dec 09 2005 12:58:00 PM'); 128.59.60.149

Anomalous Connection for



Event Details - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Event Details

Event Summary

ID	3128693
Type	Anomalous Connection
Severity	Med 85
Start Time	Dec 09 00:41 EST
Duration	1 minute

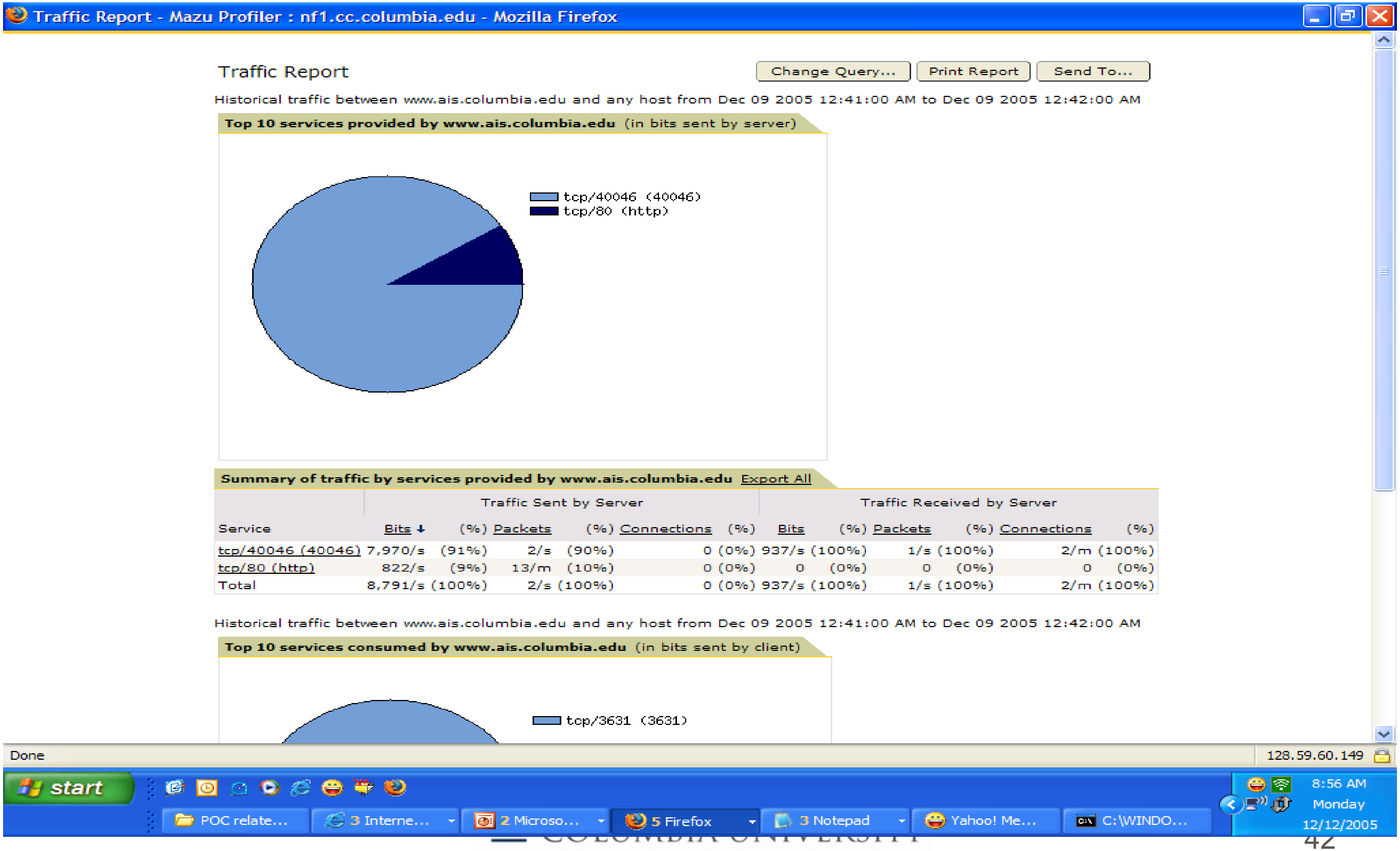
Event Details

Host being accessed (victim): 160.39.190.229.dyn.columbia.edu Morningside
Connecting host (attacker): www.ais.columbia.edu Morningside
Top Protocols: tcp(100%)
Top Services: tcp/3631(100%)

Metrics used for determining severity

Metric	Effect on Severity	Note
The attacker has not previously accessed the victim.	+20	Basic Attack.
The average host in custom group unassigned connects to 0 % of hosts in Morningside	-10	If the connection is across groups that 'rarely access each other' then severity increases by 20. If the groups 'commonly access each other' severity decreases by 10.
There were 1 TCP connections in one time period.	+5	TCP connections increase severity by 5
At least one port was not well known.	+10	If strange ports are used (above port 1024) then severity increases by 10
1 new ports were used.	+10	If a port is connected to that hasn't been connected to in the history, then severity increases by 10
There were 0 connections per second and 46 bytes per connection.	0	If there are many connections and few bytes per connection, severity is increased by 15
The victim normally receives 0 connections per second	0	If the victim normally receives more than 0.5 connections per second, severity decreases by 10
The attacker normally makes 0 connections per second.	0	If the attacker normally makes more than 0.5, severity decreases by 10
The attacker has been up for 2,642,160 seconds.	0	If the attacker has been up for less than 7 days, severity decreases by 10

Why is www.ais.columbia.edu



Traffic Report

Historical traffic between www.ais.columbia.edu and any host from Dec 09 2005 12:41:00 AM to Dec 09 2005 12:42:00 AM

Top 10 services provided by www.ais.columbia.edu (in bits sent by server)

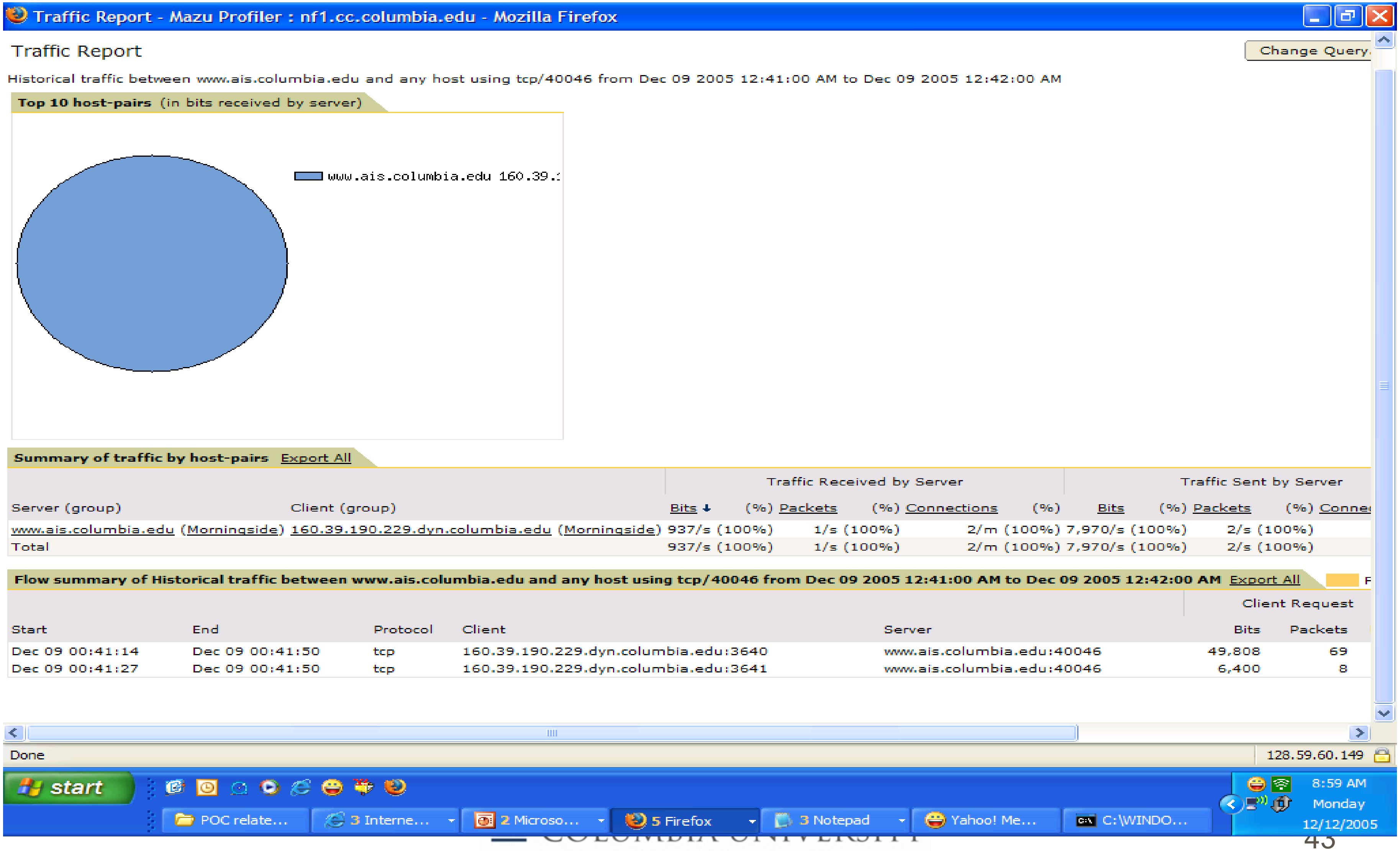
Summary of traffic by services provided by www.ais.columbia.edu Export All

	Traffic Sent by Server						Traffic Received by Server					
Service	Bits ↓	(%)	Packets	(%)	Connections	(%)	Bits	(%)	Packets	(%)	Connections	(%)
tcp/40046 (40046)	7,970/s	(91%)	2/s	(90%)	0	(0%)	937/s	(100%)	1/s	(100%)	2/m	(100%)
tcp/80 (http)	822/s	(9%)	13/m	(10%)	0	(0%)	0	(0%)	0	(0%)	0	(0%)
Total	8,791/s	(100%)	2/s	(100%)	0	(0%)	937/s	(100%)	1/s	(100%)	2/m	(100%)

Historical traffic between www.ais.columbia.edu and any host from Dec 09 2005 12:41:00 AM to Dec 09 2005 12:42:00 AM

Top 10 services consumed by www.ais.columbia.edu (in bits sent by client)

Detailed connection



Traffic Report

Historical traffic between www.ais.columbia.edu and any host using tcp/40046 from Dec 09 2005 12:41:00 AM to Dec 09 2005 12:42:00 AM

Top 10 host-pairs (in bits received by server)

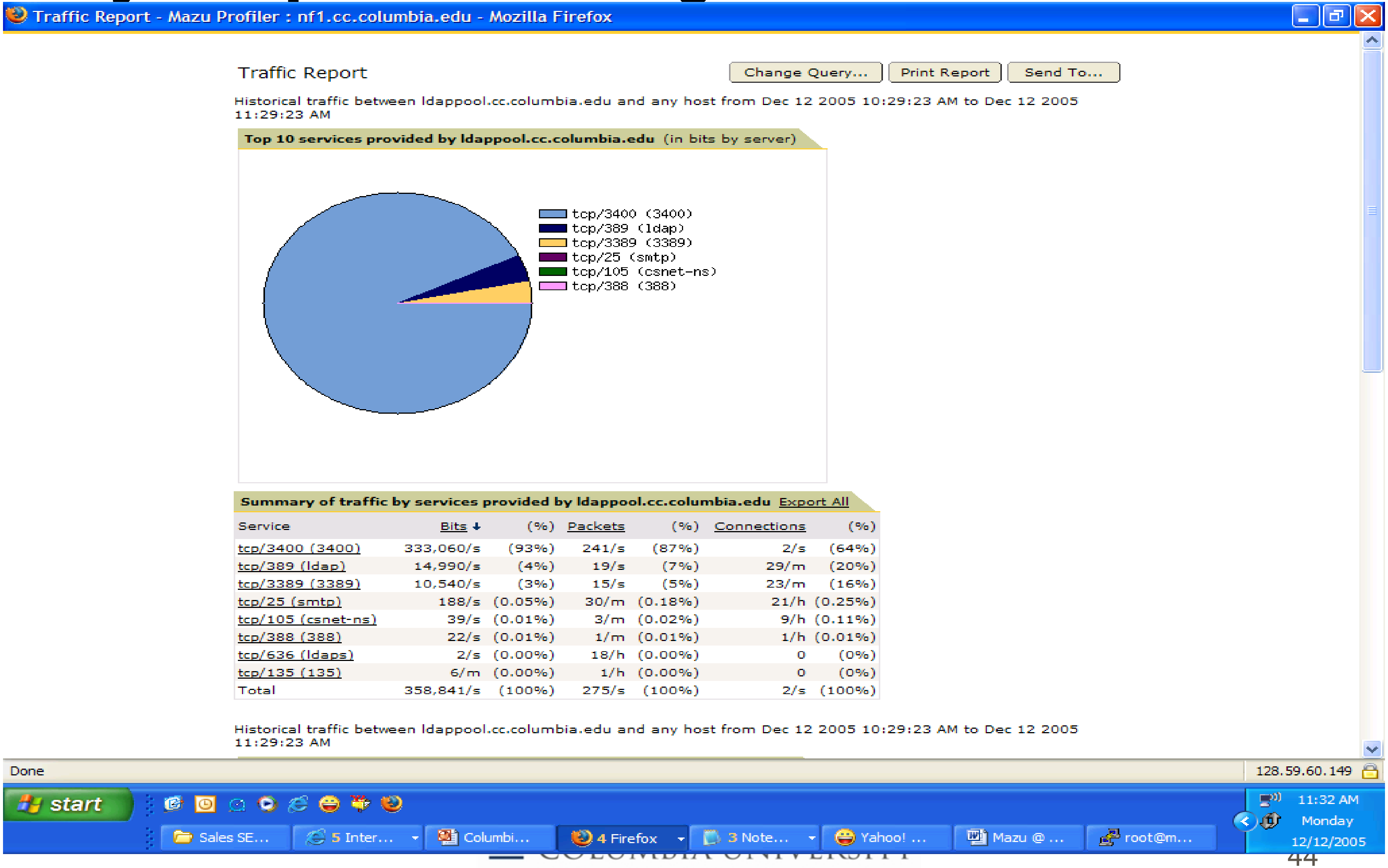
Summary of traffic by host-pairs Export All

		Traffic Received by Server						Traffic Sent by Server					
Server (group)	Client (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)	Bits	(%)	Packets	(%)	Conne	
www.ais.columbia.edu (Morningside)	160.39.190.229.dyn.columbia.edu (Morningside)	937/s	(100%)	1/s	(100%)	2/m	(100%)	7,970/s	(100%)	2/s	(100%)		
Total		937/s	(100%)	1/s	(100%)	2/m	(100%)	7,970/s	(100%)	2/s	(100%)		

Flow summary of Historical traffic between www.ais.columbia.edu and any host using tcp/40046 from Dec 09 2005 12:41:00 AM to Dec 09 2005 12:42:00 AM Export All

					Client Request	
Start	End	Protocol	Client	Server	Bits	Packets
Dec 09 00:41:14	Dec 09 00:41:50	tcp	160.39.190.229.dyn.columbia.edu:3640	www.ais.columbia.edu:40046	49,808	69
Dec 09 00:41:27	Dec 09 00:41:50	tcp	160.39.190.229.dyn.columbia.edu:3641	www.ais.columbia.edu:40046	6,400	8

Why is tcp/3400 the largest service



Traffic Report

Historical traffic between ldappool.cc.columbia.edu and any host from Dec 12 2005 10:29:23 AM to Dec 12 2005 11:29:23 AM

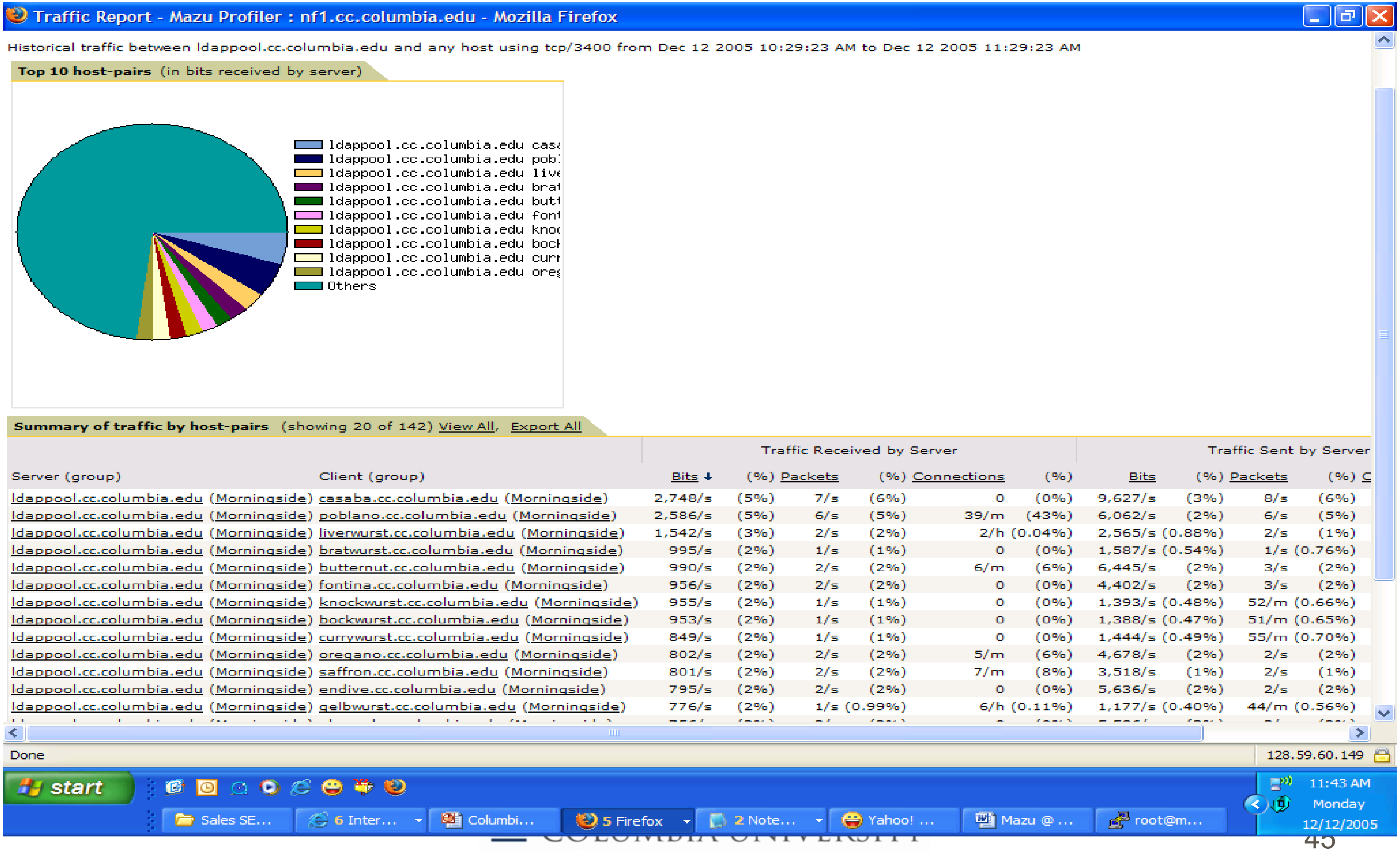
Top 10 services provided by ldappool.cc.columbia.edu (in bits by server)

Summary of traffic by services provided by ldappool.cc.columbia.edu Export All

Service	Bits ↓	(%)	Packets	(%)	Connections	(%)
tcp/3400 (3400)	333,060/s	(93%)	241/s	(87%)	2/s	(64%)
tcp/389 (ldap)	14,990/s	(4%)	19/s	(7%)	29/m	(20%)
tcp/3389 (3389)	10,540/s	(3%)	15/s	(5%)	23/m	(16%)
tcp/25 (smtp)	188/s	(0.05%)	30/m	(0.18%)	21/h	(0.25%)
tcp/105 (csnet-ns)	39/s	(0.01%)	3/m	(0.02%)	9/h	(0.11%)
tcp/388 (388)	22/s	(0.01%)	1/m	(0.01%)	1/h	(0.01%)
tcp/636 (ldaps)	2/s	(0.00%)	18/h	(0.00%)	0	(0%)
tcp/135 (135)	6/m	(0.00%)	1/h	(0.00%)	0	(0%)
Total	358,841/s	(100%)	275/s	(100%)	2/s	(100%)

Historical traffic between ldappool.cc.columbia.edu and any host from Dec 12 2005 10:29:23 AM to Dec 12 2005 11:29:23 AM

In 1-hour, 142 unique peers


Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox
ldappool.cc.columbia.edu casa
ldappool.cc.columbia.edu pobl
ldappool.cc.columbia.edu live
ldappool.cc.columbia.edu brat
ldappool.cc.columbia.edu butt
ldappool.cc.columbia.edu font
ldappool.cc.columbia.edu knoc
ldappool.cc.columbia.edu bock
ldappool.cc.columbia.edu curr
ldappool.cc.columbia.edu oreg
Others
Done
128.59.60.149
start
Sales SE...
6 Inter...
Columbi...
5 Firefox
2 Note...
Yahoo! ...
Mazu @ ...
root@m...
11:43 AM
Monday
12/12/2005

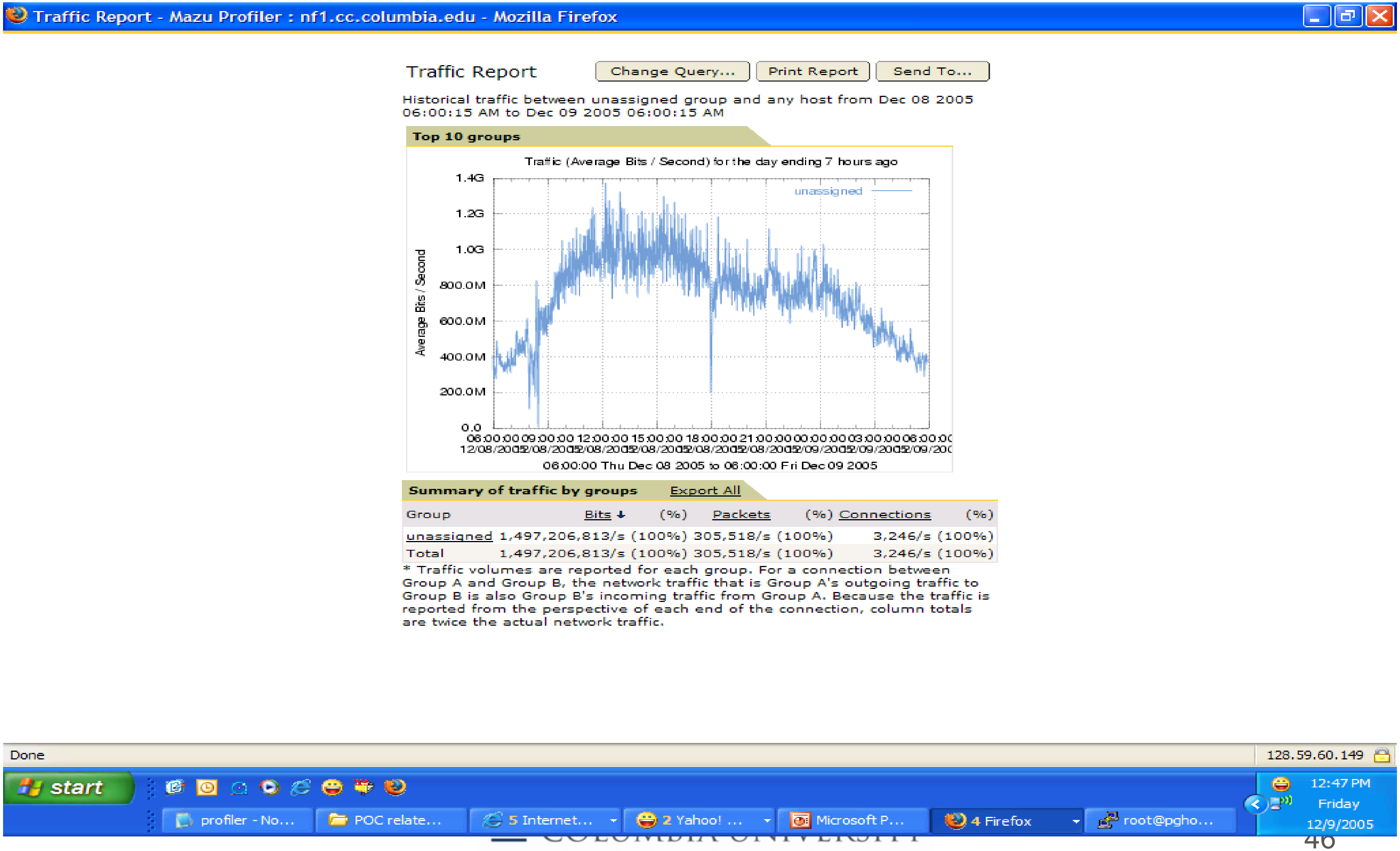
Historical traffic between ldappool.cc.columbia.edu and any host using tcp/3400 from Dec 12 2005 10:29:23 AM to Dec 12 2005 11:29:23 AM

Top 10 host-pairs (in bits received by server)

Summary of traffic by host-pairs (showing 20 of 142) View All, Export All

		Traffic Received by Server						Traffic Sent by Server				
Server (group)	Client (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)	Bits	(%)	Packets	(%)	C
ldappool.cc.columbia.edu (Morningside)	casaba.cc.columbia.edu (Morningside)	2,748/s	(5%)	7/s	(6%)	0	(0%)	9,627/s	(3%)	8/s	(6%)	
ldappool.cc.columbia.edu (Morningside)	poblano.cc.columbia.edu (Morningside)	2,586/s	(5%)	6/s	(5%)	39/m	(43%)	6,062/s	(2%)	6/s	(5%)	
ldappool.cc.columbia.edu (Morningside)	liverwurst.cc.columbia.edu (Morningside)	1,542/s	(3%)	2/s	(2%)	2/h	(0.04%)	2,565/s	(0.88%)	2/s	(1%)	
ldappool.cc.columbia.edu (Morningside)	bratwurst.cc.columbia.edu (Morningside)	995/s	(2%)	1/s	(1%)	0	(0%)	1,587/s	(0.54%)	1/s	(0.76%)	
ldappool.cc.columbia.edu (Morningside)	butternut.cc.columbia.edu (Morningside)	990/s	(2%)	2/s	(2%)	6/m	(6%)	6,445/s	(2%)	3/s	(2%)	
ldappool.cc.columbia.edu (Morningside)	fontina.cc.columbia.edu (Morningside)	956/s	(2%)	2/s	(2%)	0	(0%)	4,402/s	(2%)	3/s	(2%)	
ldappool.cc.columbia.edu (Morningside)	knockwurst.cc.columbia.edu (Morningside)	955/s	(2%)	1/s	(1%)	0	(0%)	1,393/s	(0.48%)	52/m	(0.66%)	
ldappool.cc.columbia.edu (Morningside)	bockwurst.cc.columbia.edu (Morningside)	953/s	(2%)	1/s	(1%)	0	(0%)	1,388/s	(0.47%)	51/m	(0.65%)	
ldappool.cc.columbia.edu (Morningside)	currywurst.cc.columbia.edu (Morningside)	849/s	(2%)	1/s	(1%)	0	(0%)	1,444/s	(0.49%)	55/m	(0.70%)	
ldappool.cc.columbia.edu (Morningside)	oregano.cc.columbia.edu (Morningside)	802/s	(2%)	2/s	(2%)	5/m	(6%)	4,678/s	(2%)	2/s	(2%)	
ldappool.cc.columbia.edu (Morningside)	saffron.cc.columbia.edu (Morningside)	801/s	(2%)	2/s	(2%)	7/m	(8%)	3,518/s	(1%)	2/s	(1%)	
ldappool.cc.columbia.edu (Morningside)	endive.cc.columbia.edu (Morningside)	795/s	(2%)	2/s	(2%)	0	(0%)	5,636/s	(2%)	2/s	(2%)	
ldappool.cc.columbia.edu (Morningside)	gelbwurst.cc.columbia.edu (Morningside)	776/s	(2%)	1/s	(0.99%)	6/h	(0.11%)	1,177/s	(0.40%)	44/m	(0.56%)	

Global BW



Traffic Report

Historical traffic between unassigned group and any host from Dec 08 2005 06:00:15 AM to Dec 09 2005 06:00:15 AM

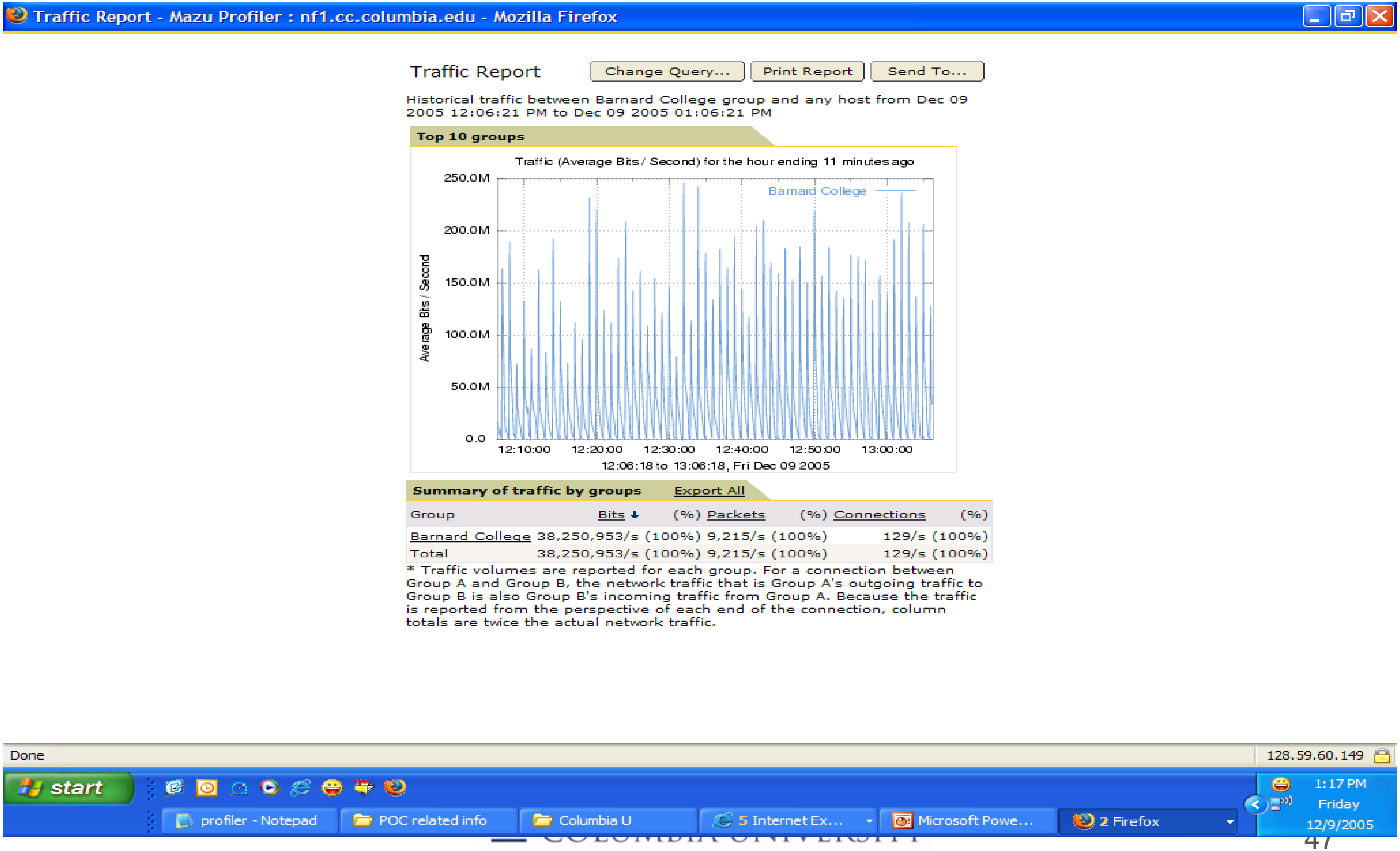
Top 10 groups

Summary of traffic by groups Export All

Group	Bits ↓	(%)	Packets	(%)	Connections	(%)
unassigned	1,497,206,813/s	(100%)	305,518/s	(100%)	3,246/s	(100%)
Total	1,497,206,813/s	(100%)	305,518/s	(100%)	3,246/s	(100%)

* Traffic volumes are reported for each group. For a connection between Group A and Group B, the network traffic that is Group A's outgoing traffic to Group B is also Group B's incoming traffic from Group A. Because the traffic is reported from the perspective of each end of the connection, column totals are twice the actual network traffic.

BW Graph for Barnard



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Traffic Report

Change Query...
Print Report
Send To...

Historical traffic between Barnard College group and any host from Dec 09 2005 12:06:21 PM to Dec 09 2005 01:06:21 PM

Top 10 groups

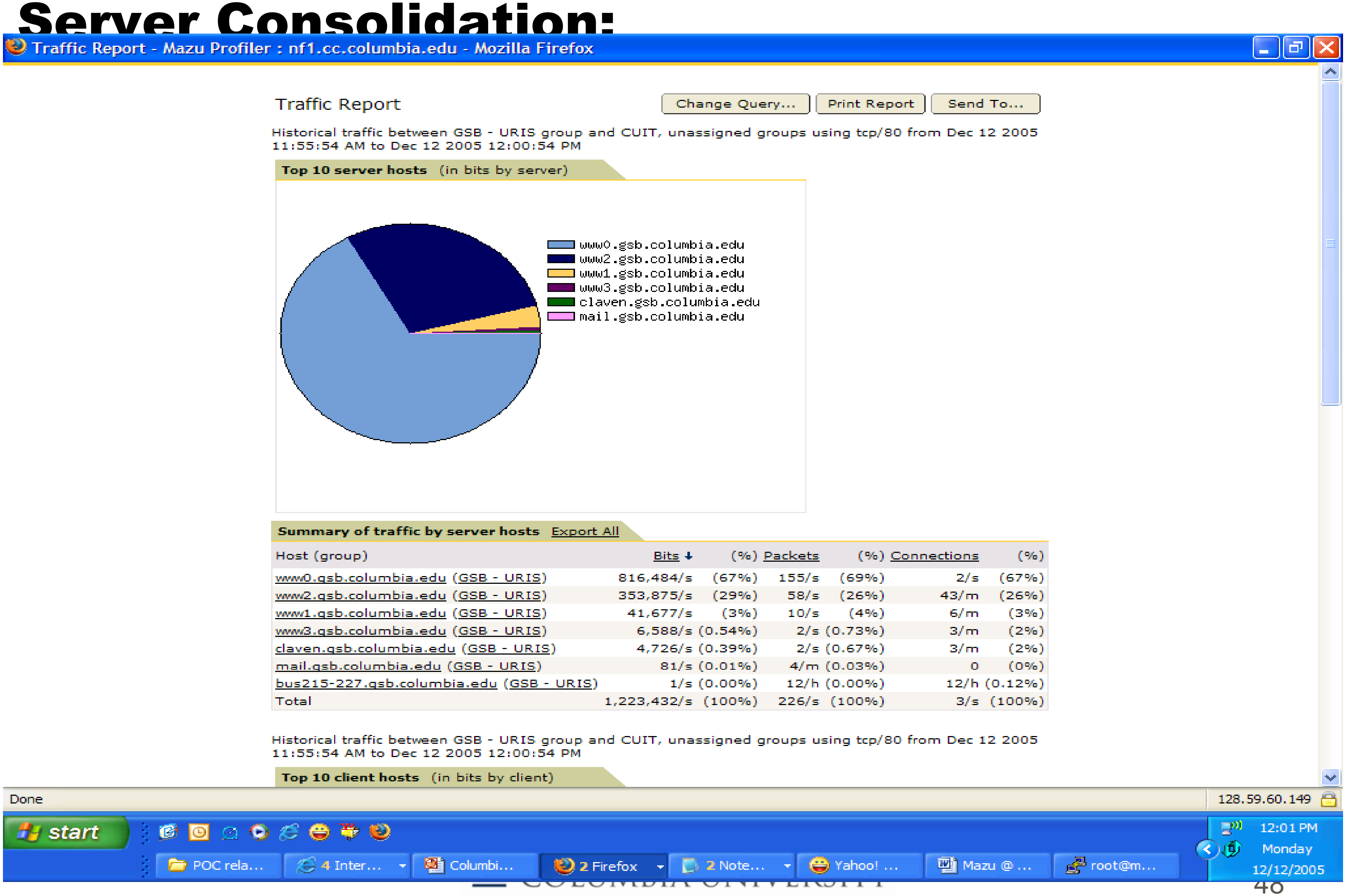
Traffic (Average Bits / Second) for the hour ending 11 minutes ago
Average Bits / Second
250.0M
200.0M
150.0M
100.0M
50.0M
0.0
12:10:00
12:20:00
12:30:00
12:40:00
12:50:00
13:00:00
12:06:18 to 13:06:18, Fri Dec 09 2005
Barnard College

Summary of traffic by groups Export All

Group	Bits ↓	(%)	Packets	(%)	Connections	(%)
Barnard College	38,250,953/s	(100%)	9,215/s	(100%)	129/s	(100%)
Total	38,250,953/s	(100%)	9,215/s	(100%)	129/s	(100%)

* Traffic volumes are reported for each group. For a connection between Group A and Group B, the network traffic that is Group A's outgoing traffic to Group B is also Group B's incoming traffic from Group A. Because the traffic is reported from the perspective of each end of the connection, column totals are twice the actual network traffic.

Server Consolidation:



Traffic Report

Historical traffic between GSB - URIS group and CUIT, unassigned groups using tcp/80 from Dec 12 2005 11:55:54 AM to Dec 12 2005 12:00:54 PM

Top 10 server hosts (in bits by server)

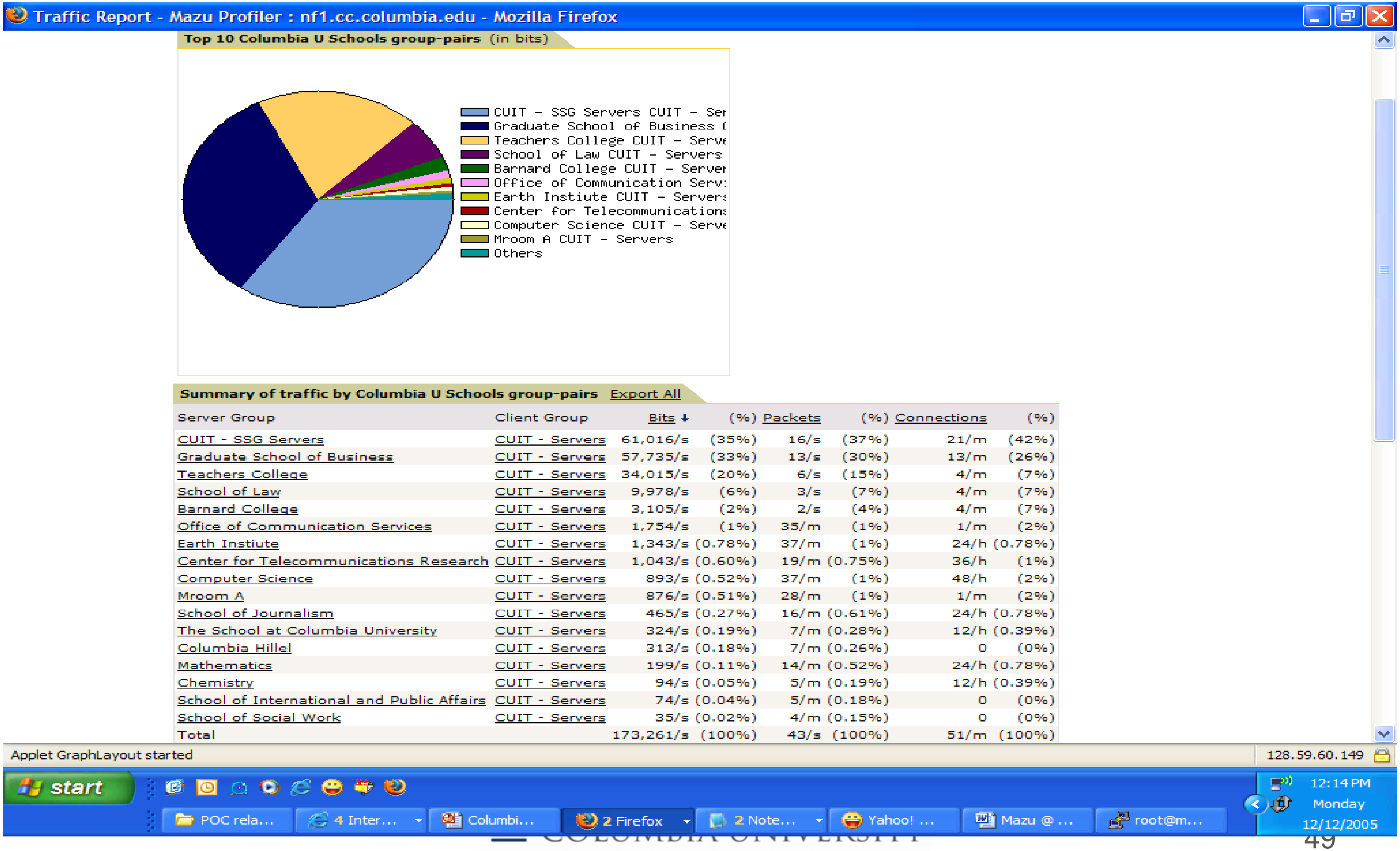
Summary of traffic by server hosts Export All

Host (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)
www0.gsb.columbia.edu (GSB - URIS)	816,484/s	(67%)	155/s	(69%)	2/s	(67%)
www2.gsb.columbia.edu (GSB - URIS)	353,875/s	(29%)	58/s	(26%)	43/m	(26%)
www1.gsb.columbia.edu (GSB - URIS)	41,677/s	(3%)	10/s	(4%)	6/m	(3%)
www3.gsb.columbia.edu (GSB - URIS)	6,588/s	(0.54%)	2/s	(0.73%)	3/m	(2%)
claven.gsb.columbia.edu (GSB - URIS)	4,726/s	(0.39%)	2/s	(0.67%)	3/m	(2%)
mail.gsb.columbia.edu (GSB - URIS)	81/s	(0.01%)	4/m	(0.03%)	0	(0%)
bus215-227.gsb.columbia.edu (GSB - URIS)	1/s	(0.00%)	12/h	(0.00%)	12/h	(0.12%)
Total	1,223,432/s	(100%)	226/s	(100%)	3/s	(100%)

Historical traffic between GSB - URIS group and CUIT, unassigned groups using tcp/80 from Dec 12 2005 11:55:54 AM to Dec 12 2005 12:00:54 PM

Top 10 client hosts (in bits by client)

Network Segmentation:



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Top 10 Columbia U Schools group-pairs (in bits)

CUIT - SSG Servers CUIT - Ser
Graduate School of Business (
Teachers College CUIT - Serve
School of Law CUIT - Servers
Barnard College CUIT - Server
Office of Communication Serv:
Earth Instiute CUIT - Servers
Center for Telecommunications
Computer Science CUIT - Serve
Mroom A CUIT - Servers
Others

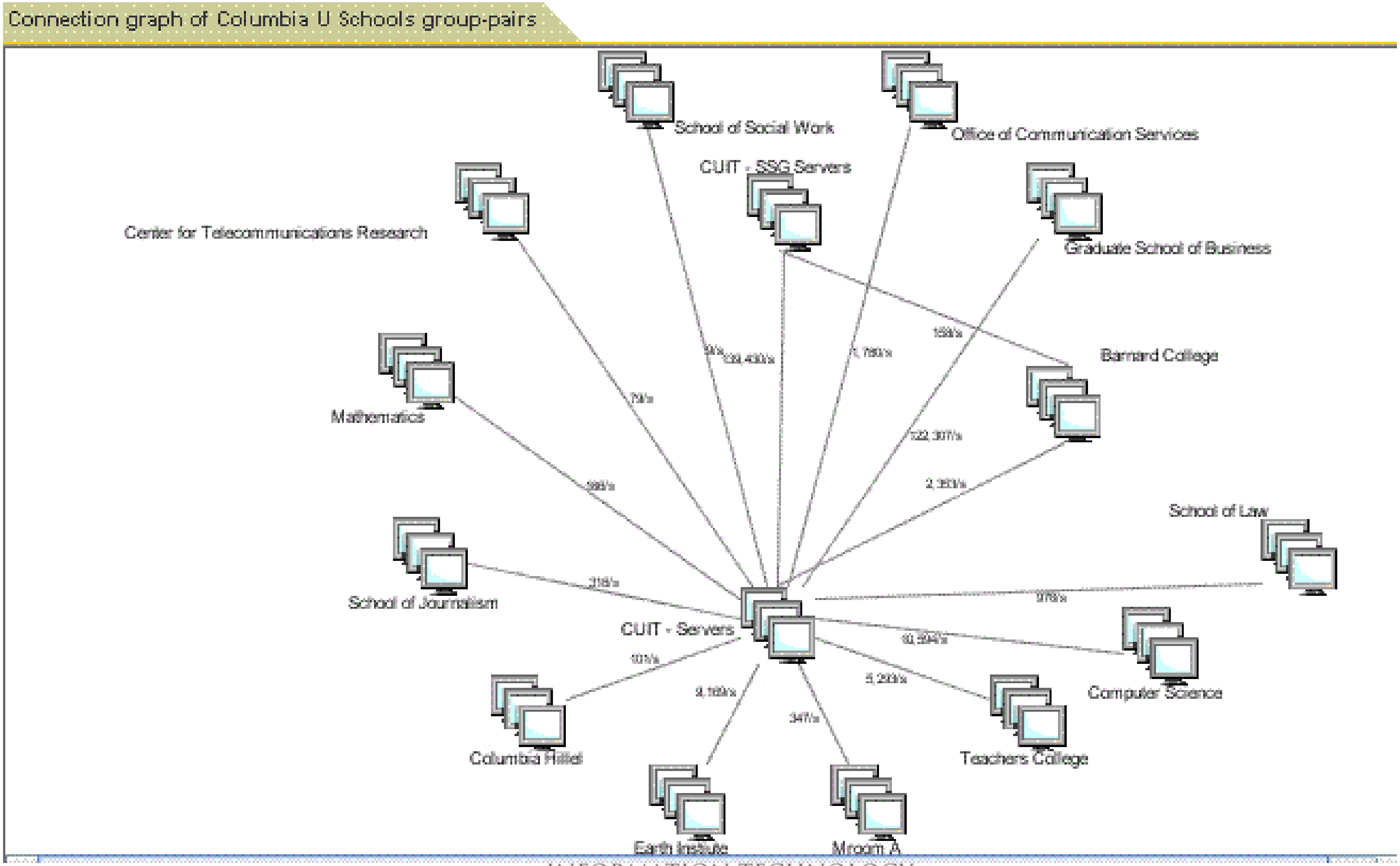
Summary of traffic by Columbia U Schools group-pairs Export All

Server Group	Client Group	Bits ↓	(%)	Packets	(%)	Connections	(%)
CUIT - SSG Servers	CUIT - Servers	61,016/s	(35%)	16/s	(37%)	21/m	(42%)
Graduate School of Business	CUIT - Servers	57,735/s	(33%)	13/s	(30%)	13/m	(26%)
Teachers College	CUIT - Servers	34,015/s	(20%)	6/s	(15%)	4/m	(7%)
School of Law	CUIT - Servers	9,978/s	(6%)	3/s	(7%)	4/m	(7%)
Barnard College	CUIT - Servers	3,105/s	(2%)	2/s	(4%)	4/m	(7%)
Office of Communication Services	CUIT - Servers	1,754/s	(1%)	35/m	(1%)	1/m	(2%)
Earth Instiute	CUIT - Servers	1,343/s	(0.78%)	37/m	(1%)	24/h	(0.78%)
Center for Telecommunications Research	CUIT - Servers	1,043/s	(0.60%)	19/m	(0.75%)	36/h	(1%)
Computer Science	CUIT - Servers	893/s	(0.52%)	37/m	(1%)	48/h	(2%)
Mroom A	CUIT - Servers	876/s	(0.51%)	28/m	(1%)	1/m	(2%)
School of Journalism	CUIT - Servers	465/s	(0.27%)	16/m	(0.61%)	24/h	(0.78%)
The School at Columbia University	CUIT - Servers	324/s	(0.19%)	7/m	(0.28%)	12/h	(0.39%)
Columbia Hillel	CUIT - Servers	313/s	(0.18%)	7/m	(0.26%)	0	(0%)
Mathematics	CUIT - Servers	199/s	(0.11%)	14/m	(0.52%)	24/h	(0.78%)
Chemistry	CUIT - Servers	94/s	(0.05%)	5/m	(0.19%)	12/h	(0.39%)
School of International and Public Affairs	CUIT - Servers	74/s	(0.04%)	5/m	(0.18%)	0	(0%)
School of Social Work	CUIT - Servers	35/s	(0.02%)	4/m	(0.15%)	0	(0%)
Total		173,261/s	(100%)	43/s	(100%)	51/m	(100%)

Applet GraphLayout started

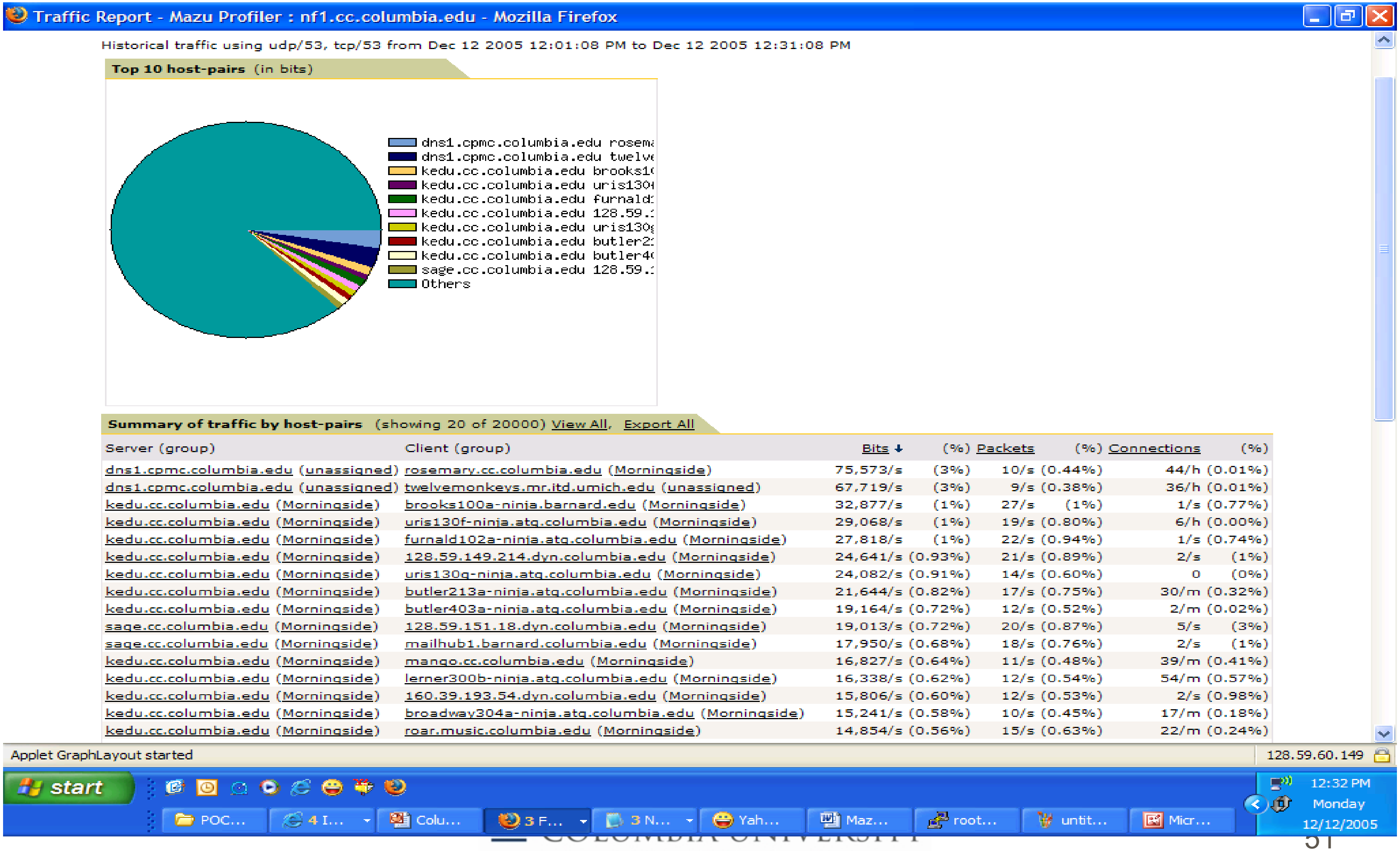
128.59.60.149

Network



Connection graph of Columbia U Schools group-pairs

Application Profiling:



Traffic Report - Mazu Profiler : nf1.cc.columbia.edu - Mozilla Firefox

Historical traffic using udp/53, tcp/53 from Dec 12 2005 12:01:08 PM to Dec 12 2005 12:31:08 PM

Top 10 host-pairs (in bits)

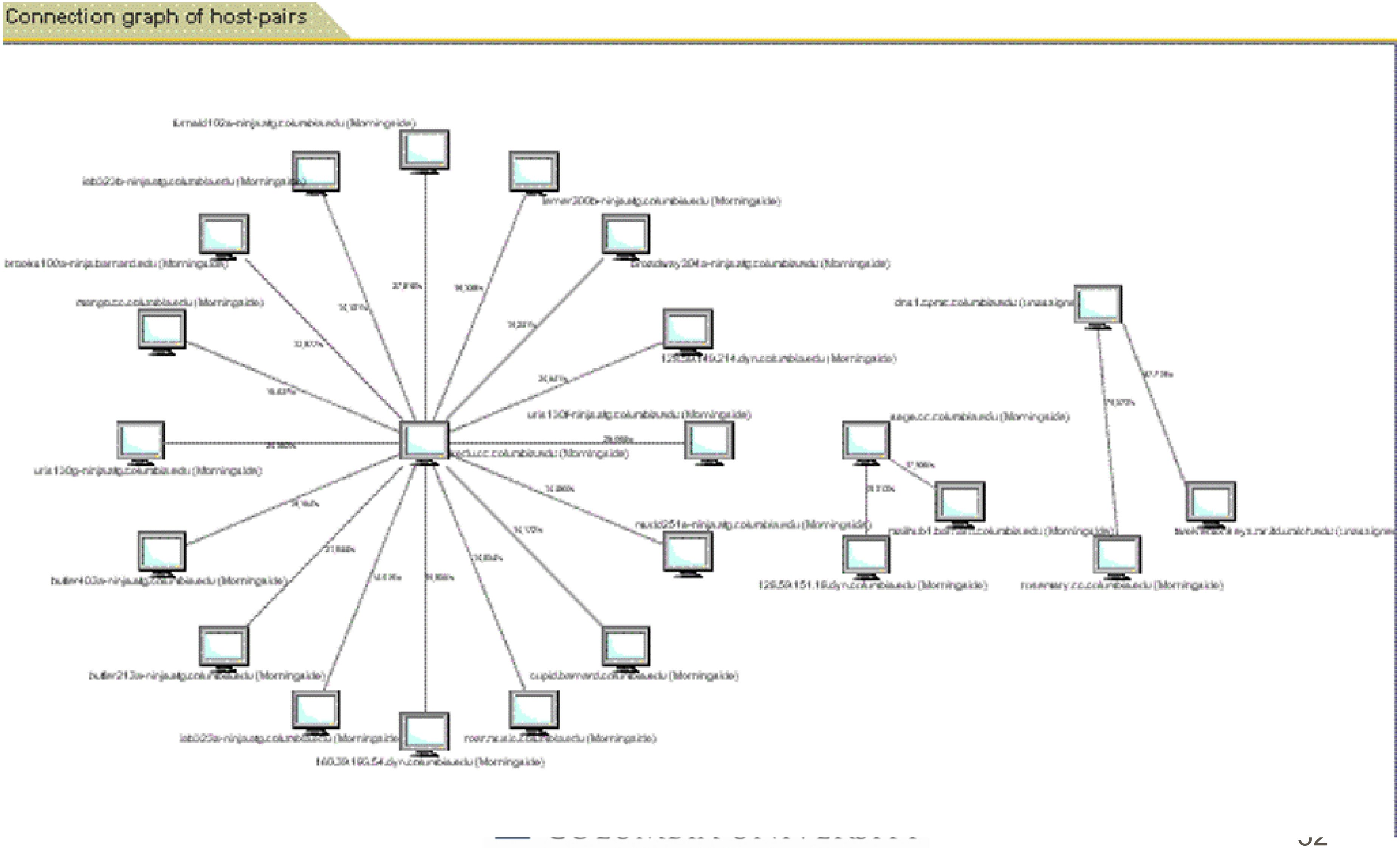
dns1.cpmc.columbia.edu rosem
dns1.cpmc.columbia.edu twelve
kedu.cc.columbia.edu brooks1
kedu.cc.columbia.edu uris130
kedu.cc.columbia.edu furnald
kedu.cc.columbia.edu 128.59.
kedu.cc.columbia.edu uris130
kedu.cc.columbia.edu butler2
kedu.cc.columbia.edu butler4
sage.cc.columbia.edu 128.59.
Others

Summary of traffic by host-pairs (showing 20 of 20000) View All, Export All

Server (group)	Client (group)	Bits ↓	(%)	Packets	(%)	Connections	(%)
dns1.cpmc.columbia.edu (unassigned)	rosemary.cc.columbia.edu (Morningside)	75,573/s	(3%)	10/s	(0.44%)	44/h	(0.01%)
dns1.cpmc.columbia.edu (unassigned)	twelvemonkeys.mr.itd.umich.edu (unassigned)	67,719/s	(3%)	9/s	(0.38%)	36/h	(0.01%)
kedu.cc.columbia.edu (Morningside)	brooks100a-ninja.barnard.edu (Morningside)	32,877/s	(1%)	27/s	(1%)	1/s	(0.77%)
kedu.cc.columbia.edu (Morningside)	uris130f-ninja.atg.columbia.edu (Morningside)	29,068/s	(1%)	19/s	(0.80%)	6/h	(0.00%)
kedu.cc.columbia.edu (Morningside)	furnald102a-ninja.atg.columbia.edu (Morningside)	27,818/s	(1%)	22/s	(0.94%)	1/s	(0.74%)
kedu.cc.columbia.edu (Morningside)	128.59.149.214.dyn.columbia.edu (Morningside)	24,641/s	(0.93%)	21/s	(0.89%)	2/s	(1%)
kedu.cc.columbia.edu (Morningside)	uris130g-ninja.atg.columbia.edu (Morningside)	24,082/s	(0.91%)	14/s	(0.60%)	0	(0%)
kedu.cc.columbia.edu (Morningside)	butler213a-ninja.atg.columbia.edu (Morningside)	21,644/s	(0.82%)	17/s	(0.75%)	30/m	(0.32%)
kedu.cc.columbia.edu (Morningside)	butler403a-ninja.atg.columbia.edu (Morningside)	19,164/s	(0.72%)	12/s	(0.52%)	2/m	(0.02%)
sage.cc.columbia.edu (Morningside)	128.59.151.18.dyn.columbia.edu (Morningside)	19,013/s	(0.72%)	20/s	(0.87%)	5/s	(3%)
sage.cc.columbia.edu (Morningside)	mailhub1.barnard.columbia.edu (Morningside)	17,950/s	(0.68%)	18/s	(0.76%)	2/s	(1%)
kedu.cc.columbia.edu (Morningside)	mango.cc.columbia.edu (Morningside)	16,827/s	(0.64%)	11/s	(0.48%)	39/m	(0.41%)
kedu.cc.columbia.edu (Morningside)	lerner300b-ninja.atg.columbia.edu (Morningside)	16,338/s	(0.62%)	12/s	(0.54%)	54/m	(0.57%)
kedu.cc.columbia.edu (Morningside)	160.39.193.54.dyn.columbia.edu (Morningside)	15,806/s	(0.60%)	12/s	(0.53%)	2/s	(0.98%)
kedu.cc.columbia.edu (Morningside)	broadway304a-ninja.atg.columbia.edu (Morningside)	15,241/s	(0.58%)	10/s	(0.45%)	17/m	(0.18%)
kedu.cc.columbia.edu (Morningside)	roar.music.columbia.edu (Morningside)	14,854/s	(0.56%)	15/s	(0.63%)	22/m	(0.24%)

Applet GraphLayout started

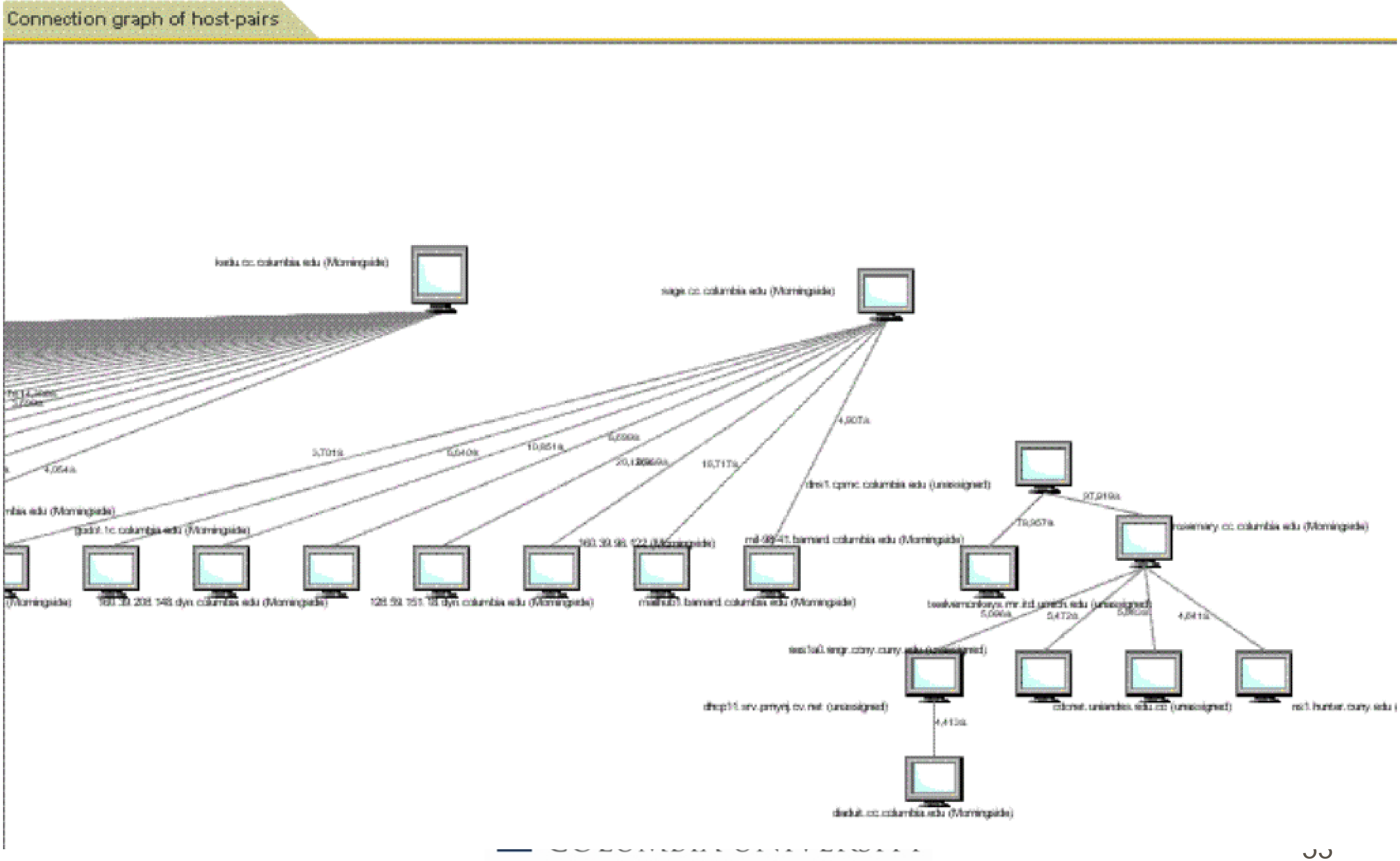
Application



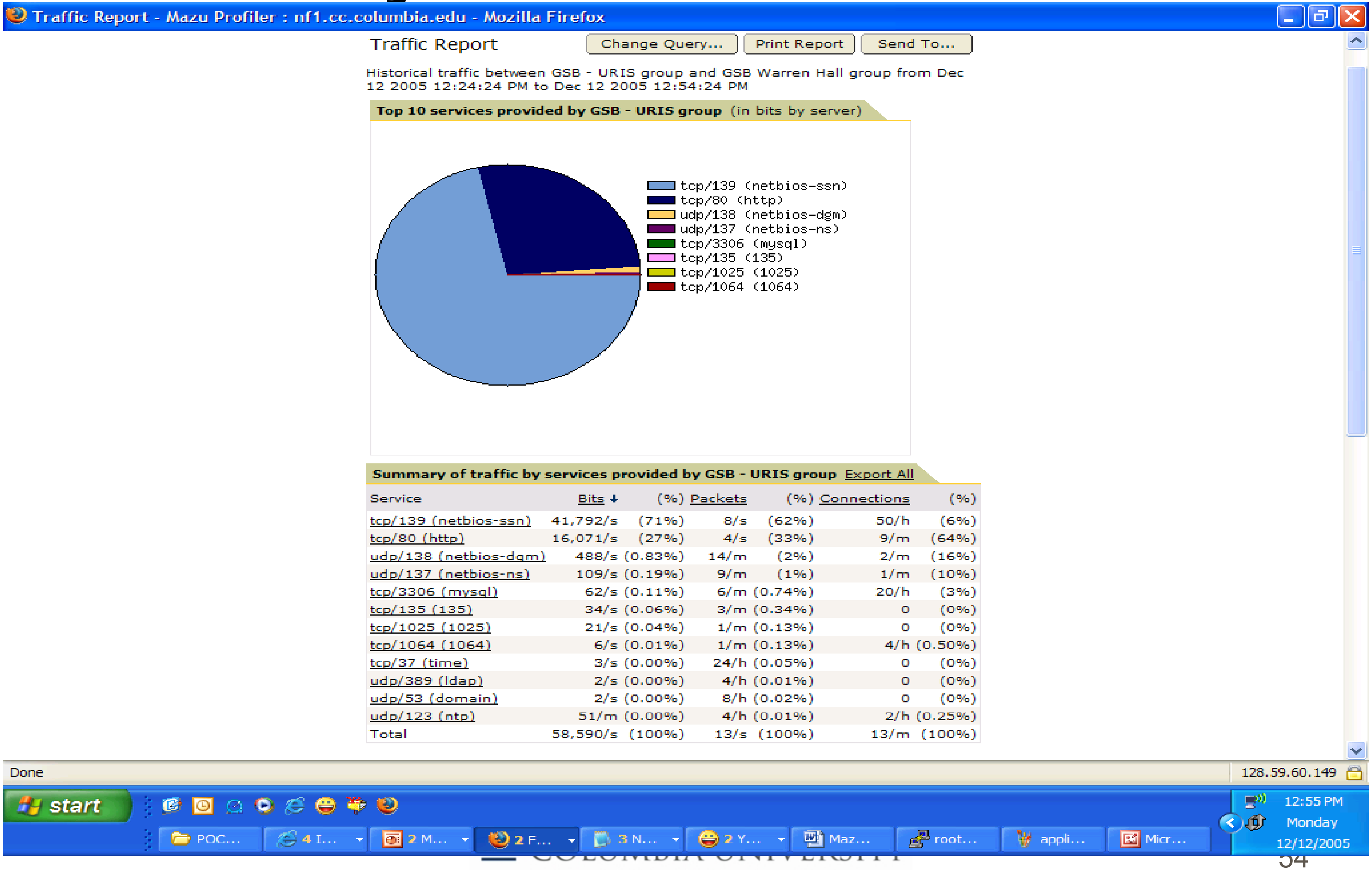
Connection graph of host-pairs

lionald102a-ninja.atg.columbia.edu (Morningside)
lab023b-ninja.atg.columbia.edu (Morningside)
lerner200b-ninja.atg.columbia.edu (Morningside)
brooks100a-ninja.barnard.edu (Morningside)
broadway304a-ninja.atg.columbia.edu (Morningside)
mango.cc.columbia.edu (Morningside)
128.59.149.214.dyn.columbia.edu (Morningside)
uris130f-ninja.atg.columbia.edu (Morningside)
uris130g-ninja.atg.columbia.edu (Morningside)
perl.cc.columbia.edu (Morningside)
music251a-ninja.atg.columbia.edu (Morningside)
butler403a-ninja.atg.columbia.edu (Morningside)
butler213a-ninja.atg.columbia.edu (Morningside)
cupid.barnard.columbia.edu (Morningside)
lab023a-ninja.atg.columbia.edu (Morningside)
roar.music.columbia.edu (Morningside)
160.39.190.54.dyn.columbia.edu (Morningside)
dns1.cpmc.columbia.edu (unassigned)
sage.cc.columbia.edu (Morningside)
mailhub1.barnard.columbia.edu (Morningside)
128.59.151.16.dyn.columbia.edu (Morningside)
rosemary.cc.columbia.edu (Morningside)
37.108%

Application


Connection graph of host-pairs
kedu.cc.columbia.edu (Morningside)
sage.cc.columbia.edu (Morningside)
4,064s
3,701s
5,640s
10,851s
5,699s
20,136s
16,717s
4,907s
mbia.edu (Morningside)
godot.1c.columbia.edu (Morningside)
(Morningside)
160.39.208.148.dyn.columbia.edu (Morningside)
128.59.151.18.dyn.columbia.edu (Morningside)
160.39.98.122 (Morningside)
mailhub1.barnard.columbia.edu (Morningside)
mil-98-41.barnard.columbia.edu (Morningside)
dns1.cpmc.columbia.edu (unassigned)
97,919s
19,957s
rosemary.cc.columbia.edu (Morningside)
twelvemonkeys.mr.itd.umich.edu (unassigned)
5,096s
5,472s
5,860s
4,841s
esc1a0.engr.ccny.cuny.edu (unassigned)
dhcp11.srv.pmynj.cv.net (unassigned)
colcnet.uniandes.edu.co (unassigned)
ns1.hunter.cuny.edu
4,413s
diaduit.cc.columbia.edu (Morningside)

Access Policy for GSB: Services



Traffic Report

Historical traffic between GSB - URIS group and GSB Warren Hall group from Dec 12 2005 12:24:24 PM to Dec 12 2005 12:54:24 PM

Top 10 services provided by GSB - URIS group (in bits by server)

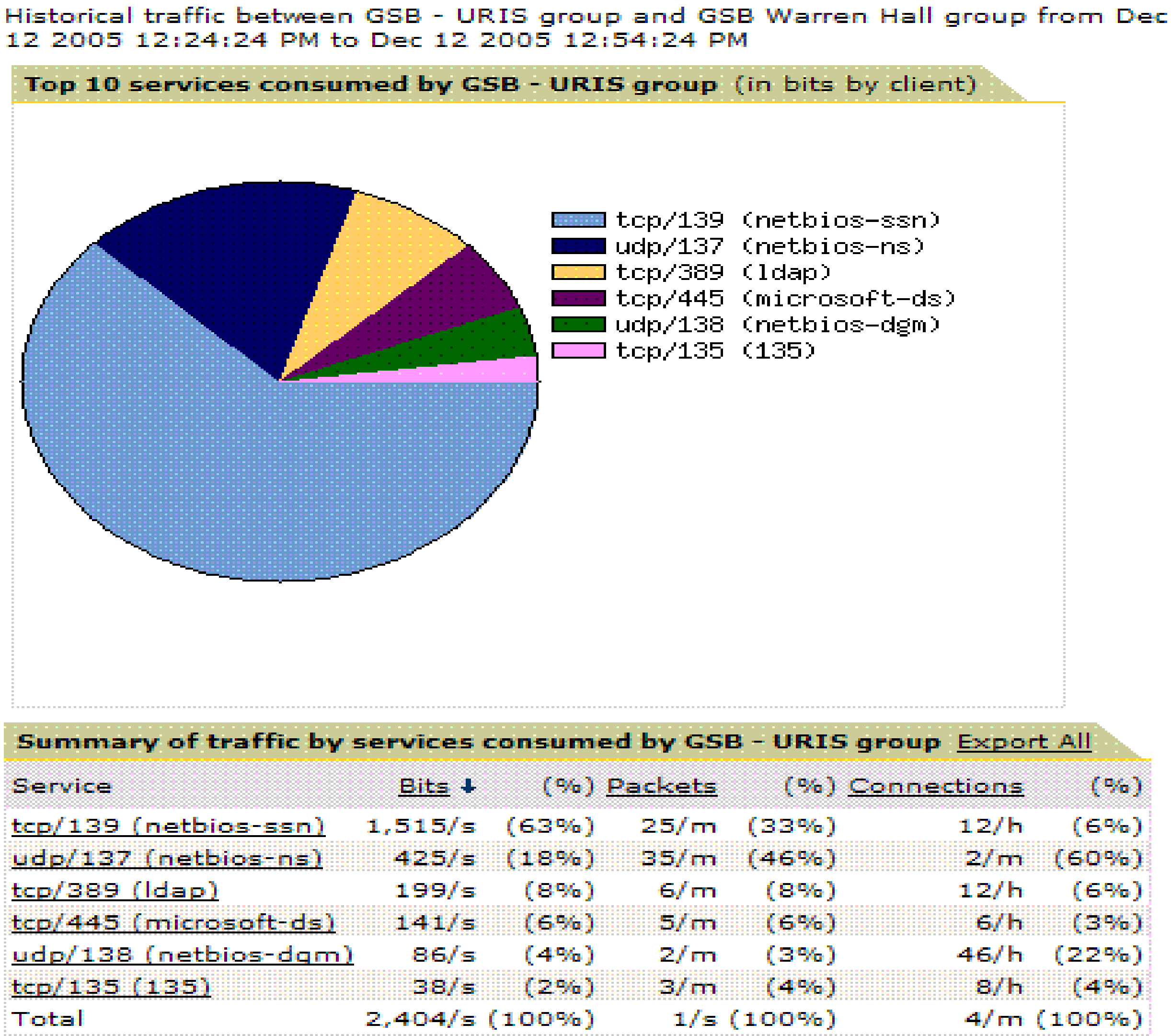
Summary of traffic by services provided by GSB - URIS group Export All

Service	Bits ↓	(%)	Packets	(%)	Connections	(%)
tcp/139 (netbios-ssn)	41,792/s	(71%)	8/s	(62%)	50/h	(6%)
tcp/80 (http)	16,071/s	(27%)	4/s	(33%)	9/m	(64%)
udp/138 (netbios-dgm)	488/s	(0.83%)	14/m	(2%)	2/m	(16%)
udp/137 (netbios-ns)	109/s	(0.19%)	9/m	(1%)	1/m	(10%)
tcp/3306 (mysql)	62/s	(0.11%)	6/m	(0.74%)	20/h	(3%)
tcp/135 (135)	34/s	(0.06%)	3/m	(0.34%)	0	(0%)
tcp/1025 (1025)	21/s	(0.04%)	1/m	(0.13%)	0	(0%)
tcp/1064 (1064)	6/s	(0.01%)	1/m	(0.13%)	4/h	(0.50%)
tcp/37 (time)	3/s	(0.00%)	24/h	(0.05%)	0	(0%)
udp/389 (ldap)	2/s	(0.00%)	4/h	(0.01%)	0	(0%)
udp/53 (domain)	2/s	(0.00%)	8/h	(0.02%)	0	(0%)
udp/123 (ntp)	51/m	(0.00%)	4/h	(0.01%)	2/h	(0.25%)
Total	58,590/s	(100%)	13/s	(100%)	13/m	(100%)

Access Policy for GSB: Services

I

I



Historical traffic between GSB - URIS group and GSB Warren Hall group from Dec 12 2005 12:24:24 PM to Dec 12 2005 12:54:24 PM

Top 10 services consumed by GSB - URIS group (in bits by client)

Summary of traffic by services consumed by GSB - URIS group Export All

Service	Bits ↓	(%)	Packets	(%)	Connections	(%)
tcp/139 (netbios-ssn)	1,515/s	(63%)	25/m	(33%)	12/h	(6%)
udp/137 (netbios-ns)	425/s	(18%)	35/m	(46%)	2/m	(60%)
tcp/389 (ldap)	199/s	(8%)	6/m	(8%)	12/h	(6%)
tcp/445 (microsoft-ds)	141/s	(6%)	5/m	(6%)	6/h	(3%)
udp/138 (netbios-dgm)	86/s	(4%)	2/m	(3%)	46/h	(22%)
tcp/135 (135)	38/s	(2%)	3/m	(4%)	8/h	(4%)
Total	2,404/s	(100%)	1/s	(100%)	4/m	(100%)