Network Analysis with iSiLK

Presented at FloCon® 2011

Ron Bandes
CERT® Network Situational Awareness (NetSA) Group

Overview

Network Monitoring

Packets and Flows

Collection, Packing, Repository, and Analysis

SiLK vs. iSiLK

Live CD (OK, it’s a DVD)

Starting iSiLK and running a query

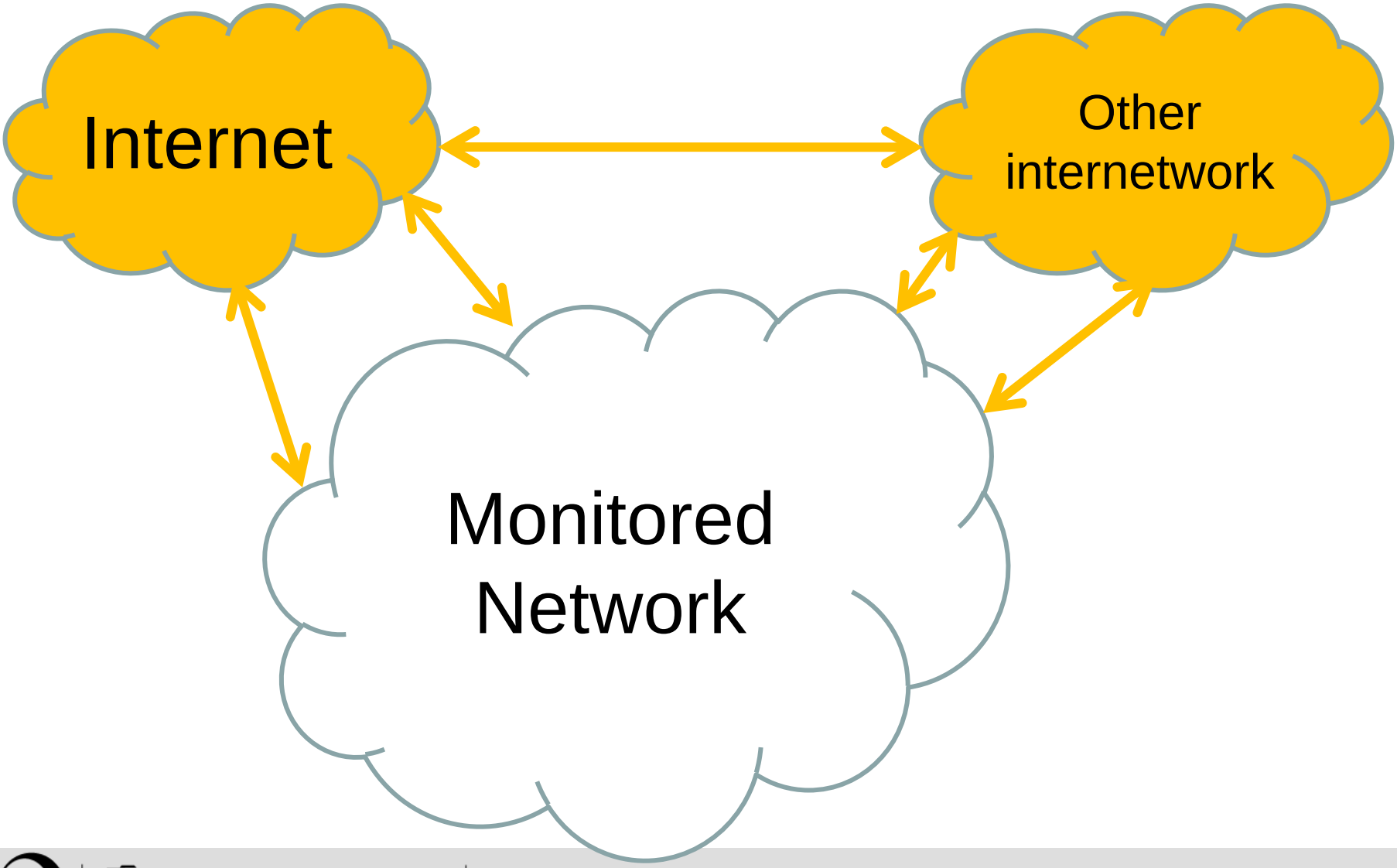
Demo: Query, summarize, refine query, summarize, report

Lab

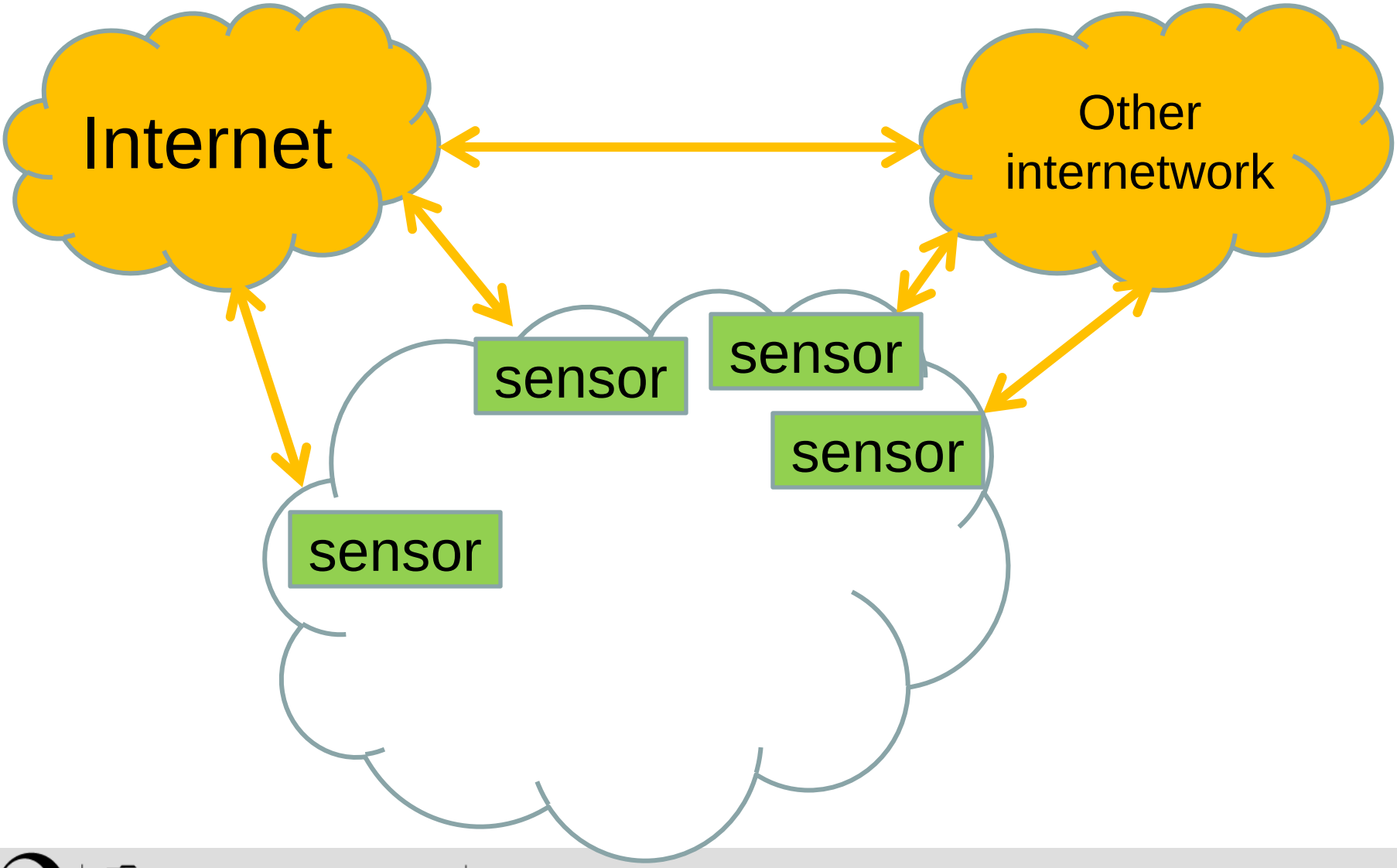
What is iSiLK?

It is a graphical front-end for SiLK,
the System for Internet Level Knowledge
flow analysis tool

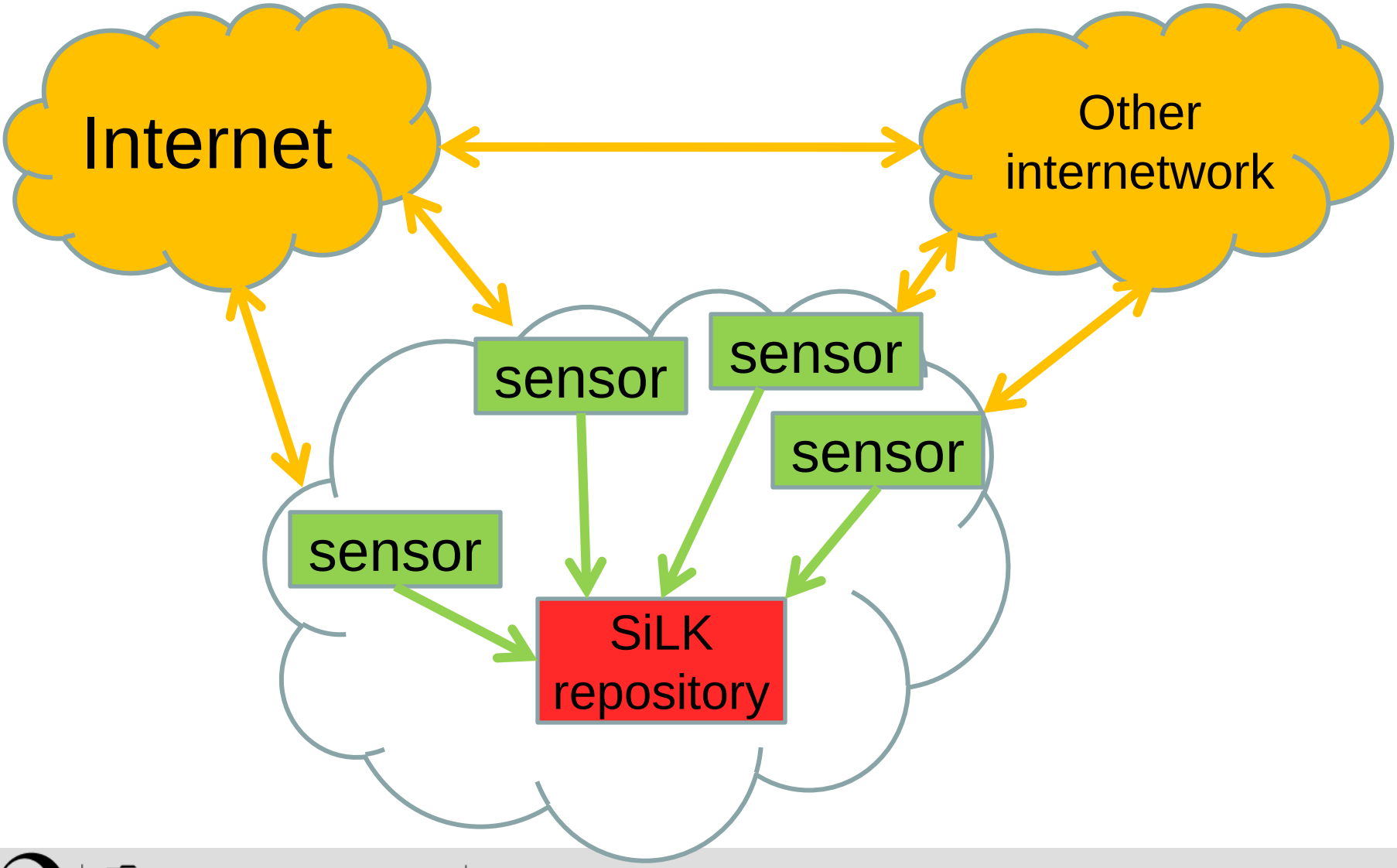
Network Monitoring



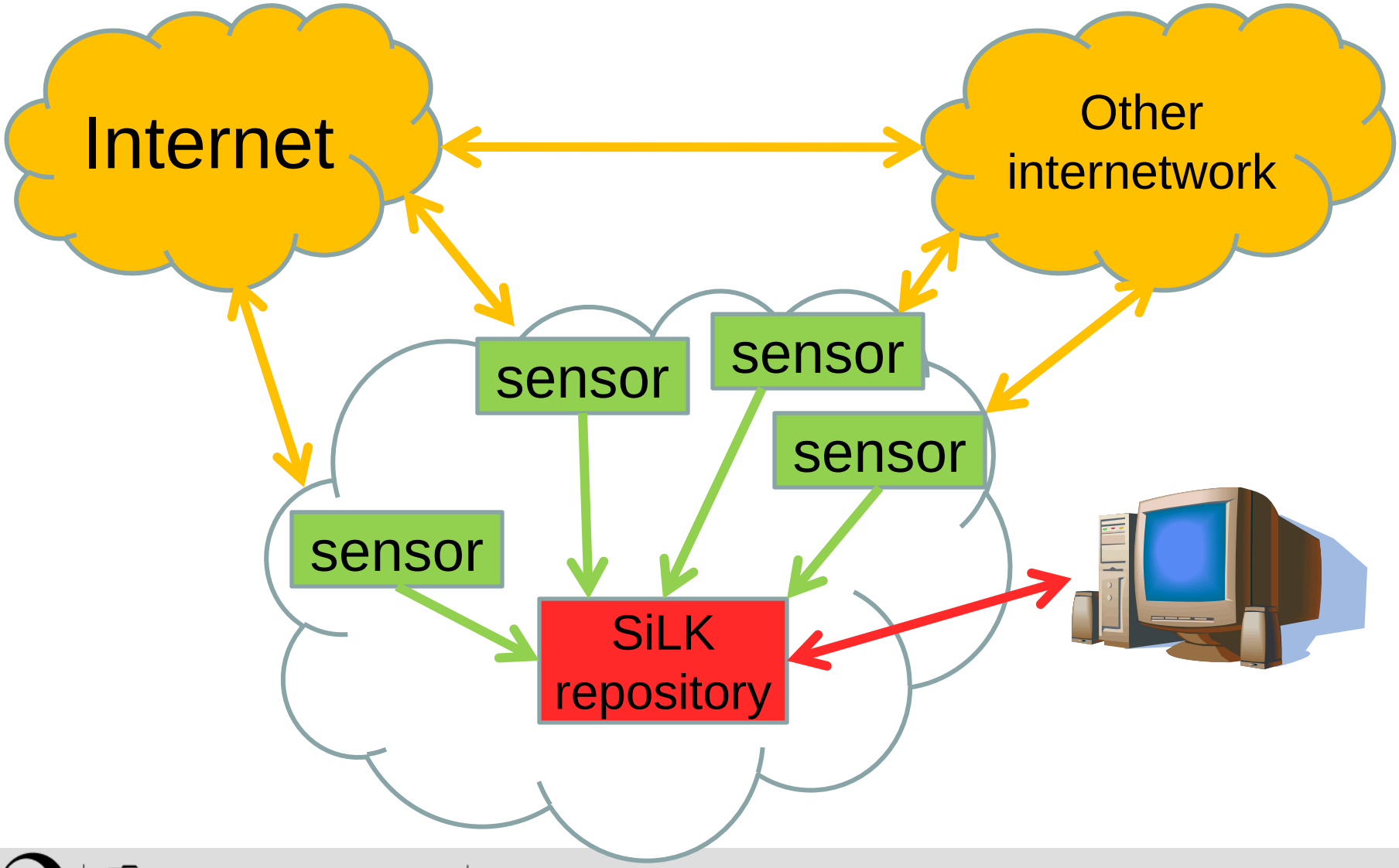
Network Monitoring



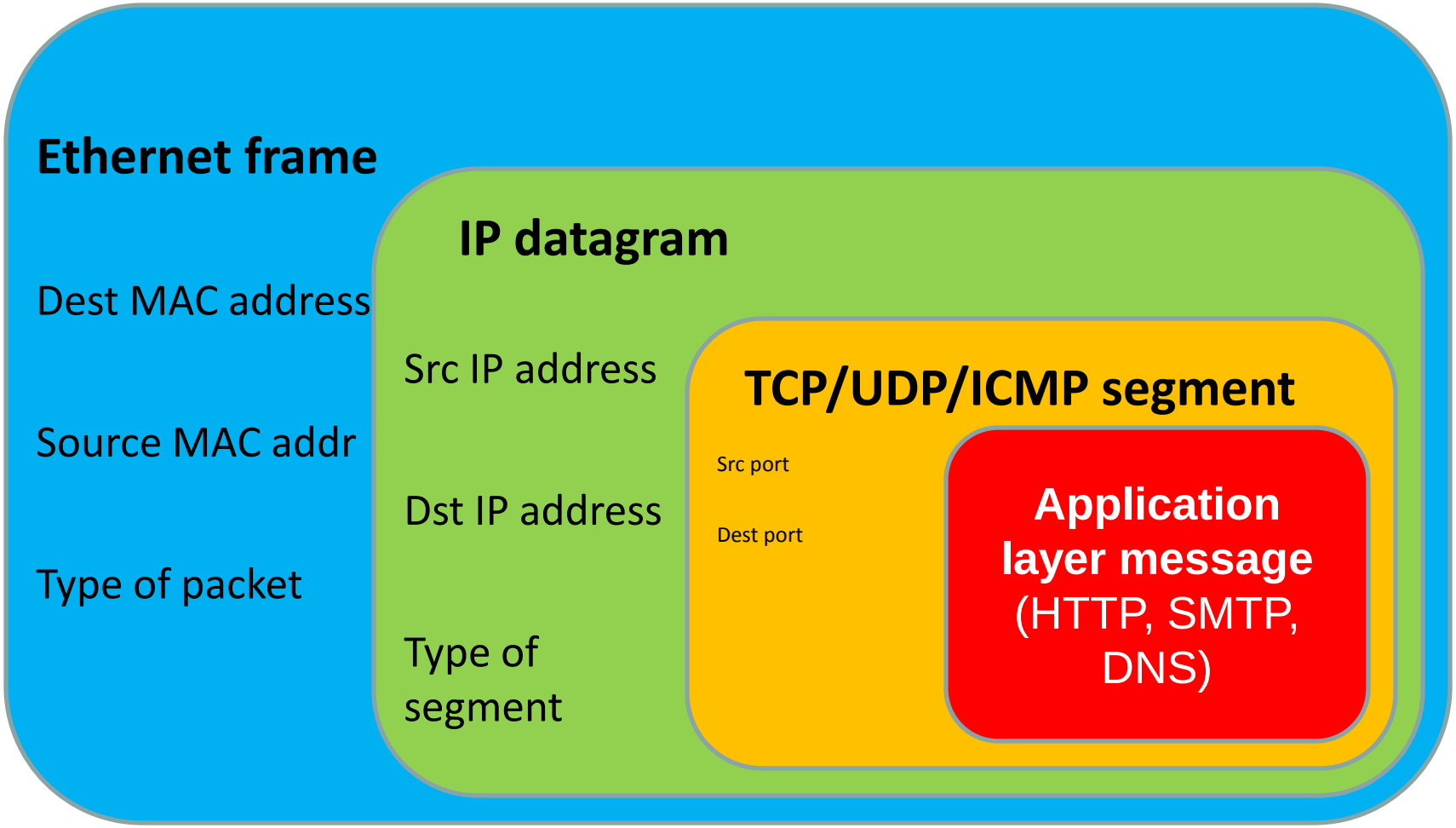
Network Monitoring



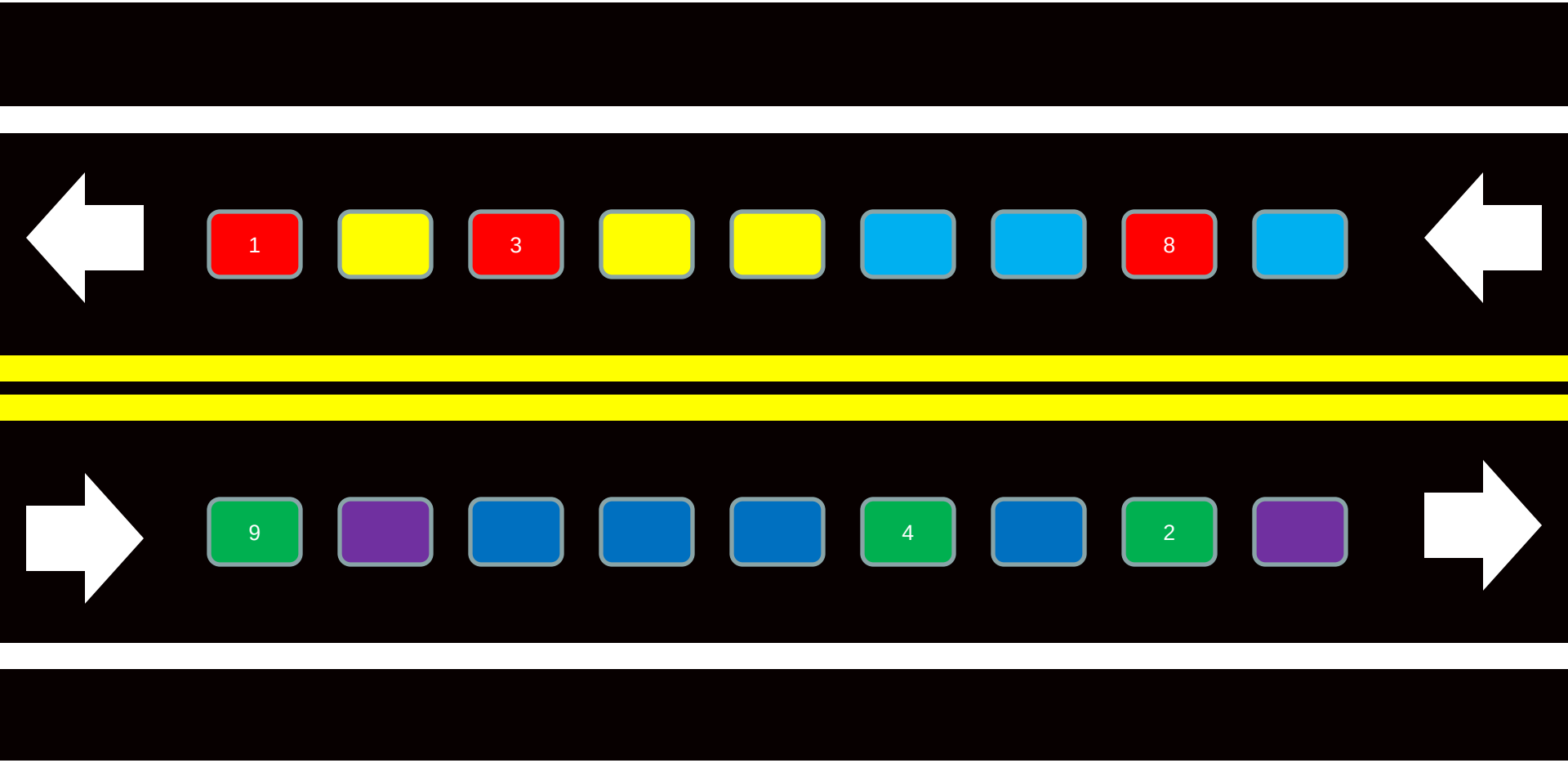
Network Monitoring



Packet Encapsulation



Flows



Some Terms

SiLK: A traffic analysis tool which processes flow data.

Flow: the collection of packets travelling in the same direction in a TCP or UDP connection.

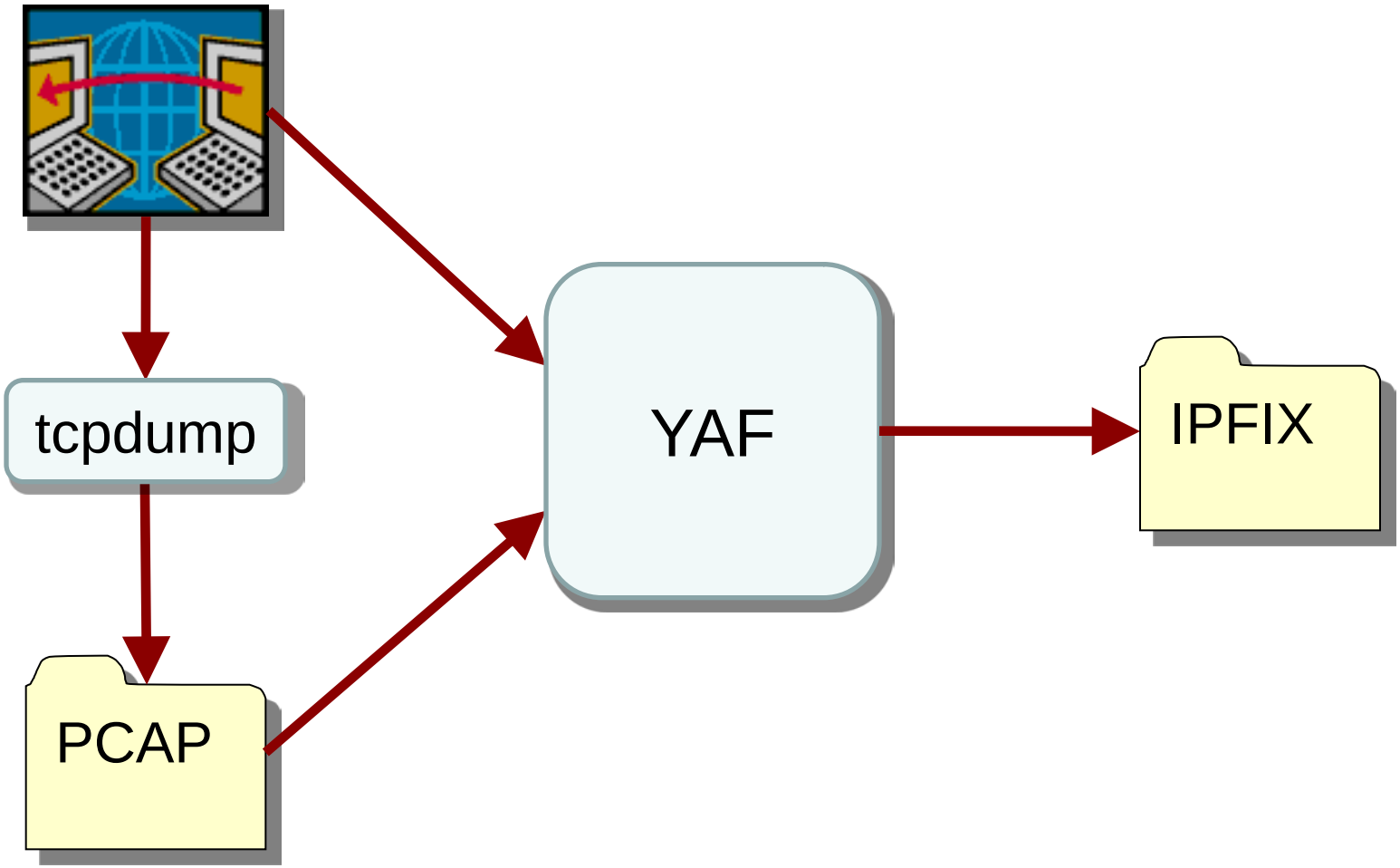
Flow Record: a single record containing summary information for a flow.

Flow Repository: a tree structure of flat files containing flow records.

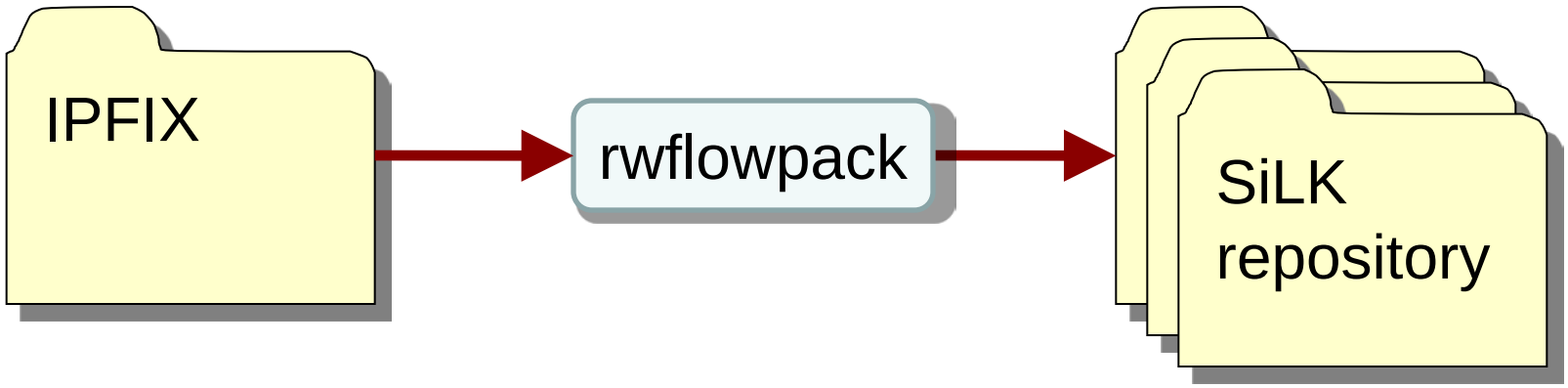
Collection, Packing, and Analysis

- **Collection** of flow data
  - Examines packets and summarizes into standard flow records
  - Timeout and payload-size values are established during collection
- **Packing** stores flow records in a scheme optimized for space and ease of analysis
- **Analysis** of flow data
  - Investigation of flow records using SiLK tools

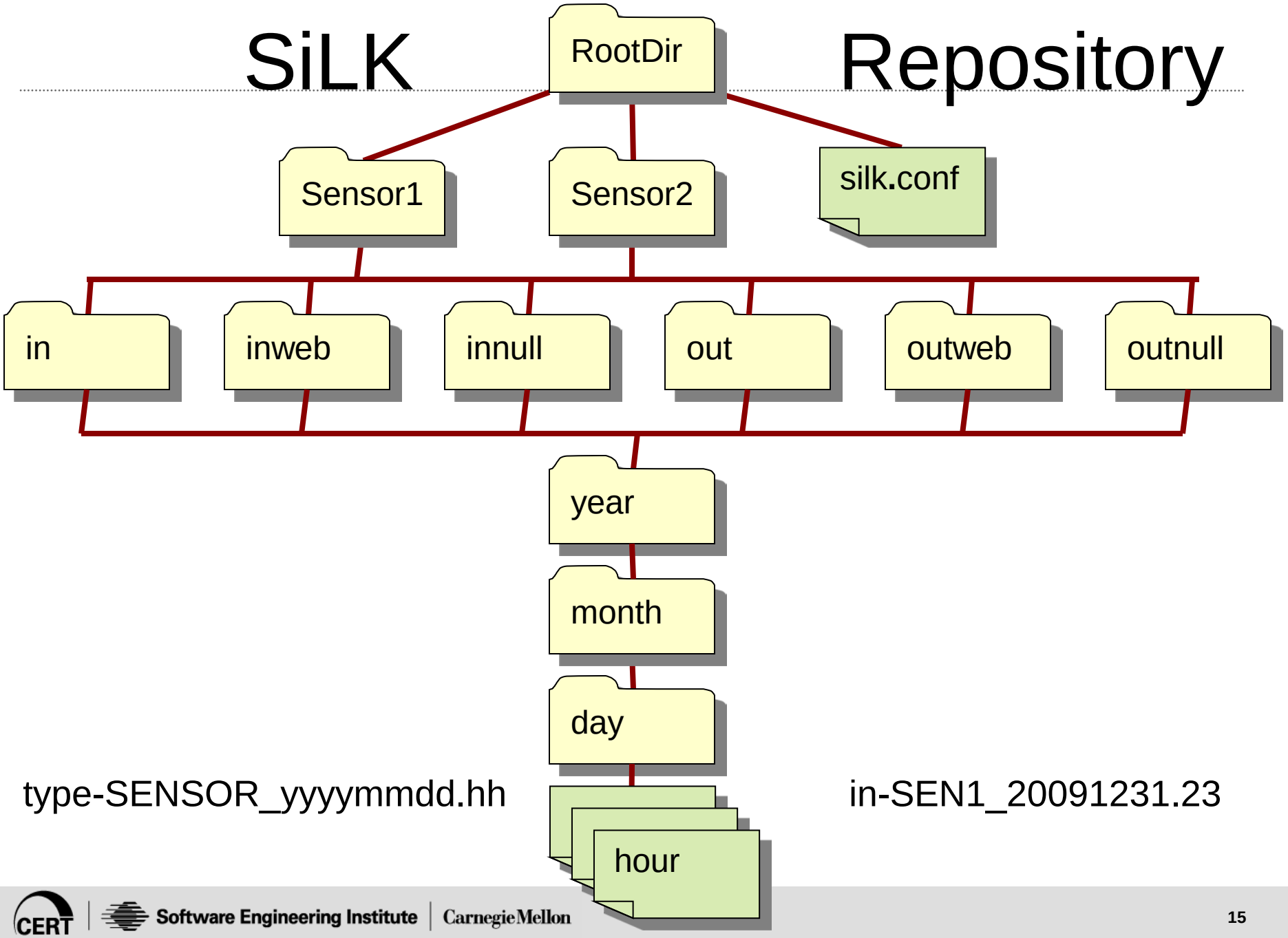
Collection



Packing



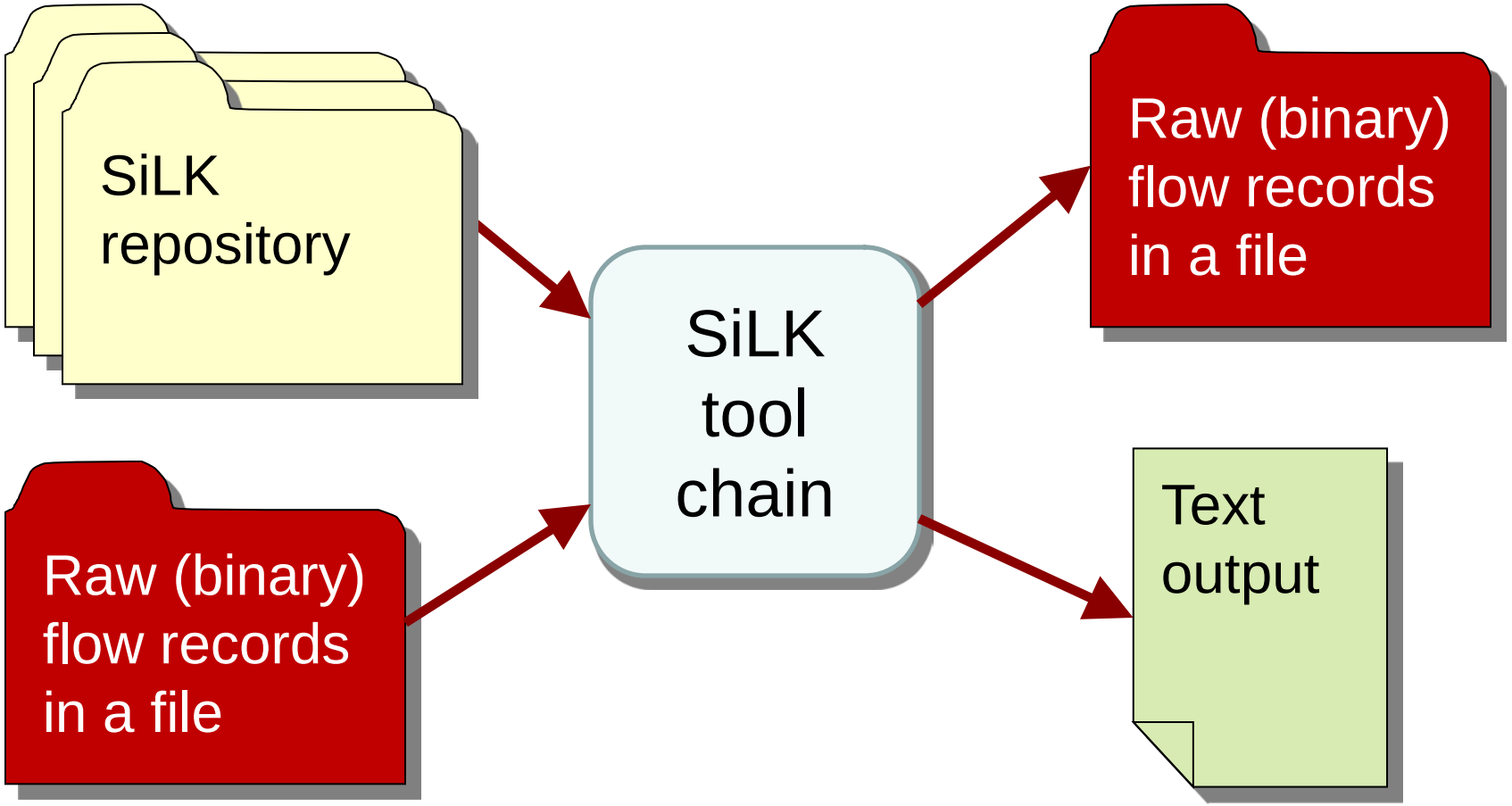
SiLK Repository



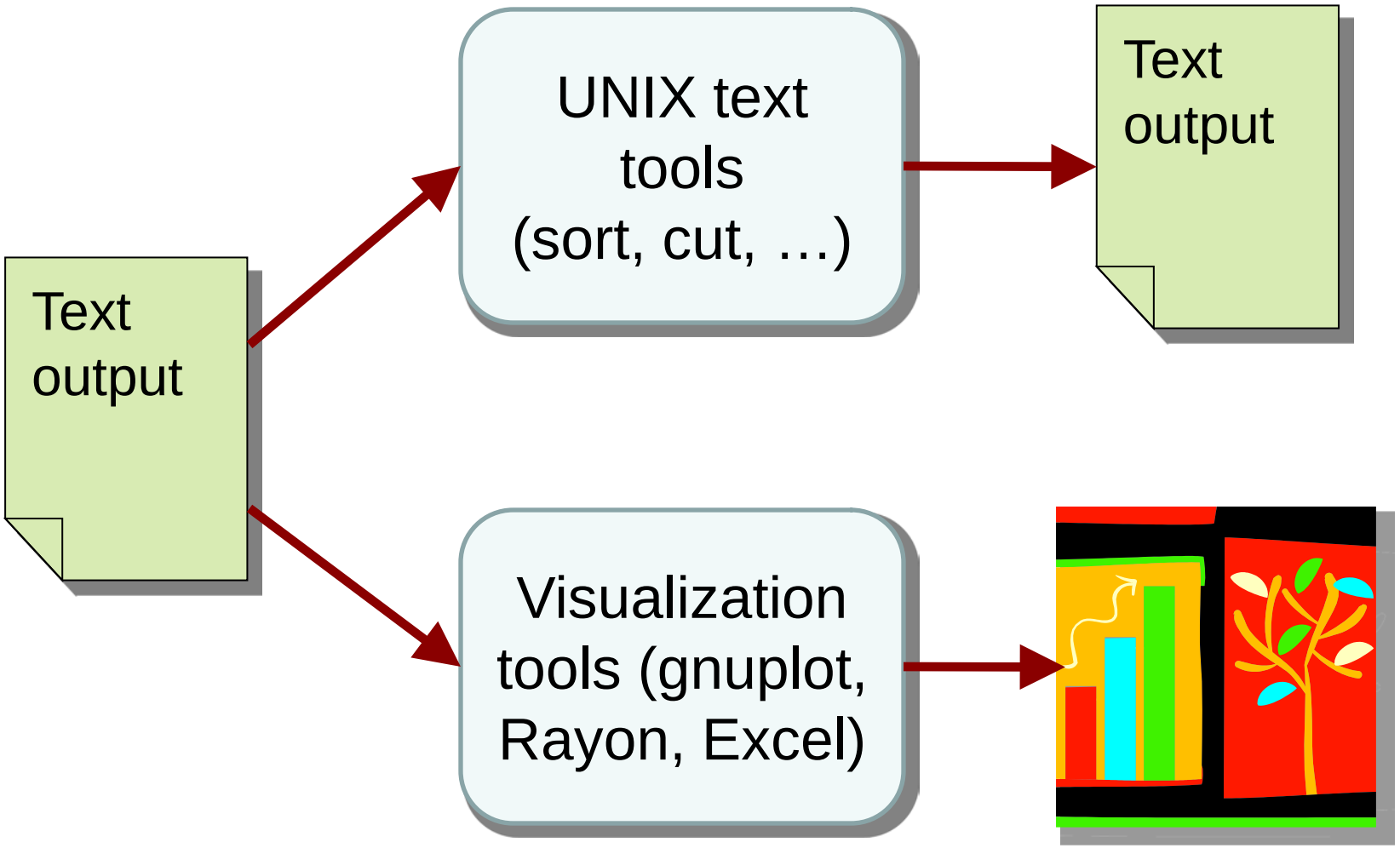
type-SENSOR_yyyymmdd.hh

in-SEN1_20091231.23

Analysis


SiLK repository
Raw (binary) flow records in a file
SiLK tool chain
Raw (binary) flow records in a file
Text output

Reporting


Text output
UNIX text tools (sort, cut, …)
Text output
Visualization tools (gnuplot, Rayon, Excel)

Why use iSiLK?

It helps me to choose SiLK tools

- Toolbar buttons allow quick perusal of tools

It lets me avoid SiLK tool syntax

- Menus & other GUI elements show my choices

It lets me avoid Linux command syntax and file names

- iSiLK organizes my data sets and results

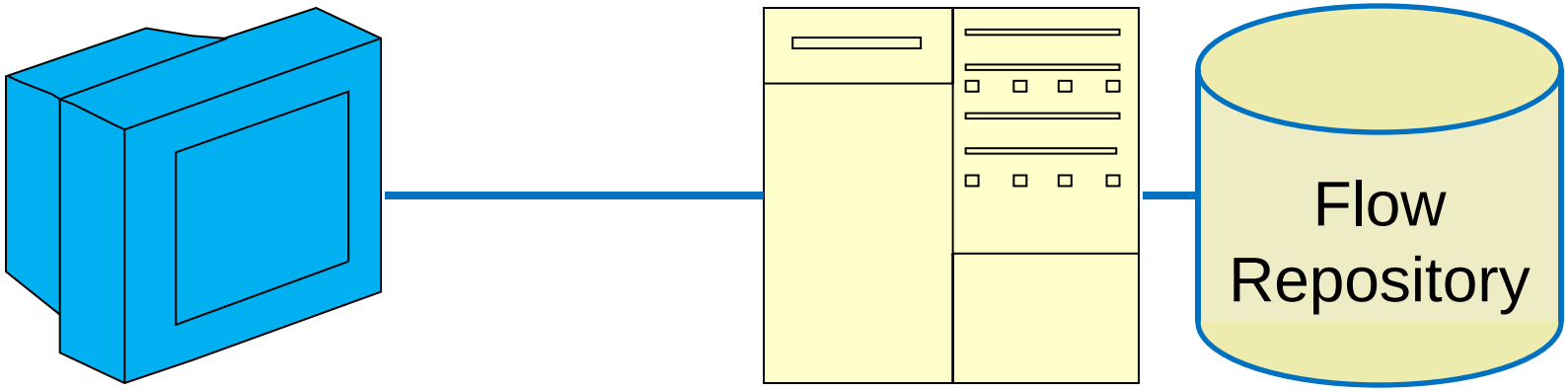
It has an integrated graphing capability

What won’t iSiLK do?

iSiLK won’t replace my need to understand what’s in flow data

I still need to understand what patterns in flow data represent the traffic situations that I’m looking for

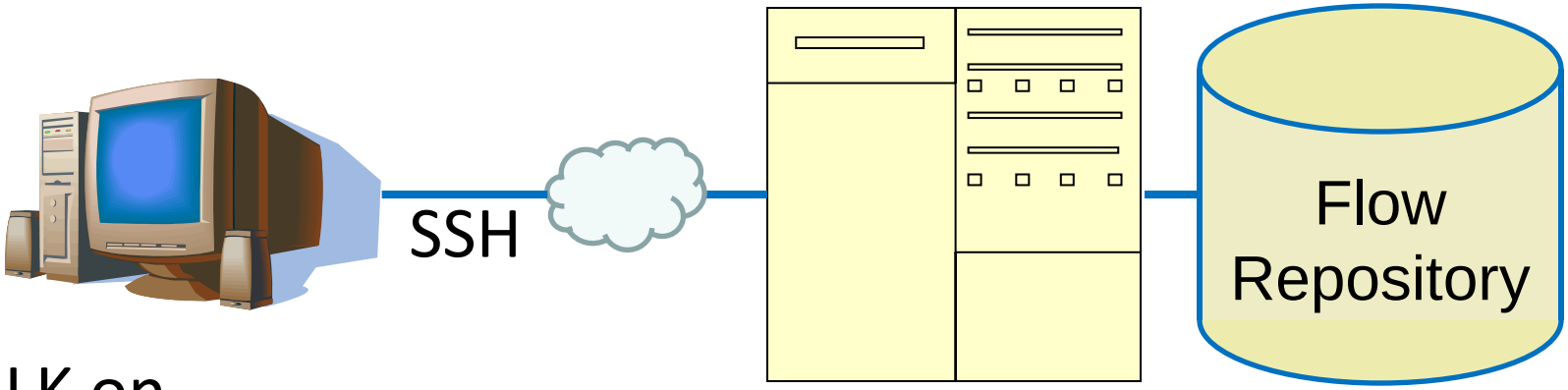
SiLK environment



Terminal window

SiLK on Linux system

iSiLK environment



iSiLK on
Windows system
(or Mac or Linux)

SiLK on
Linux system

Setting up iSiLK on the Live CD

Open Applications→System Tools →Terminal

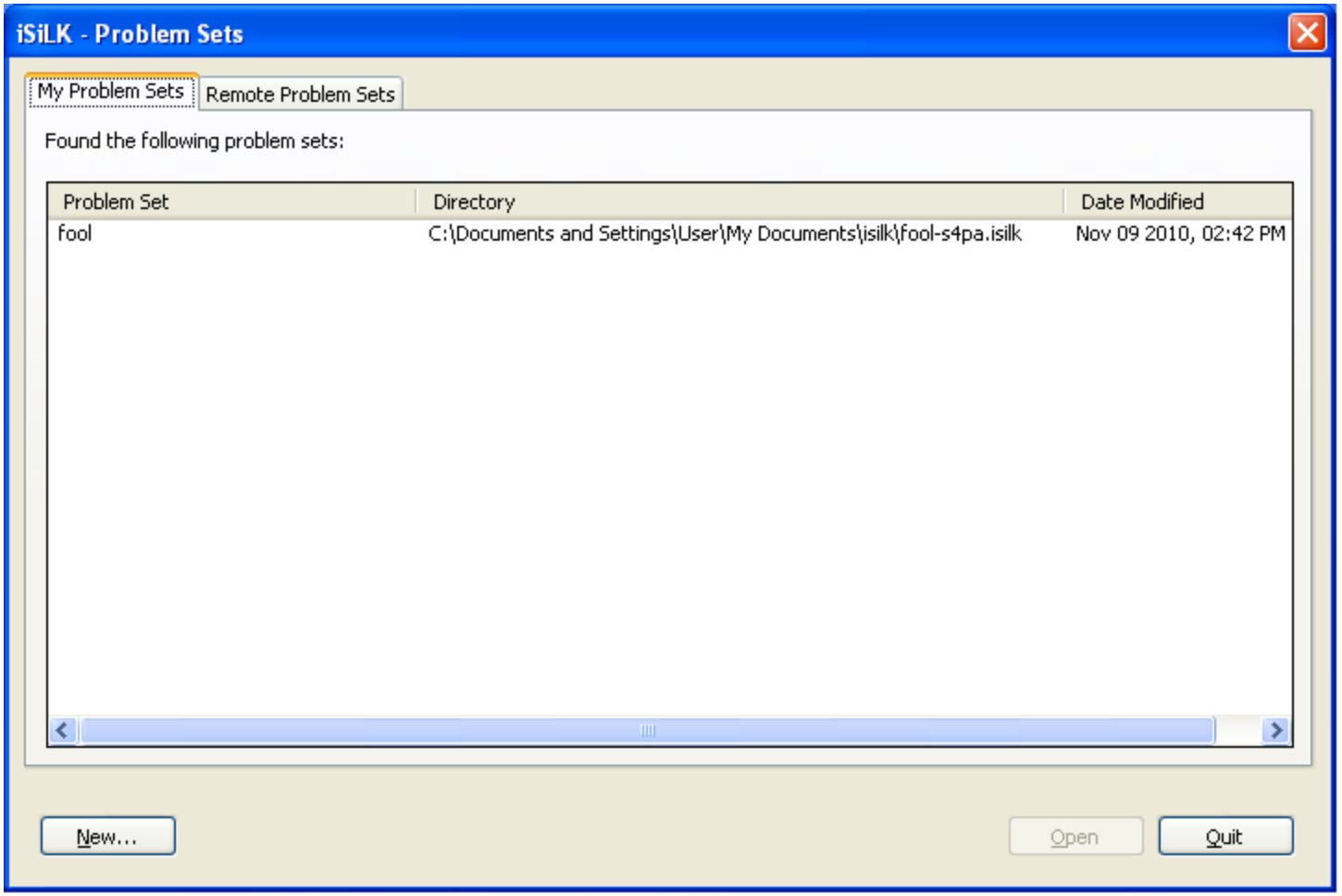
echo "export SILK_DATA_ROOTDIR=/data/SiLK-LBNL-05" >>.bashrc

On the desktop, open Applications →Programming →iSiLK

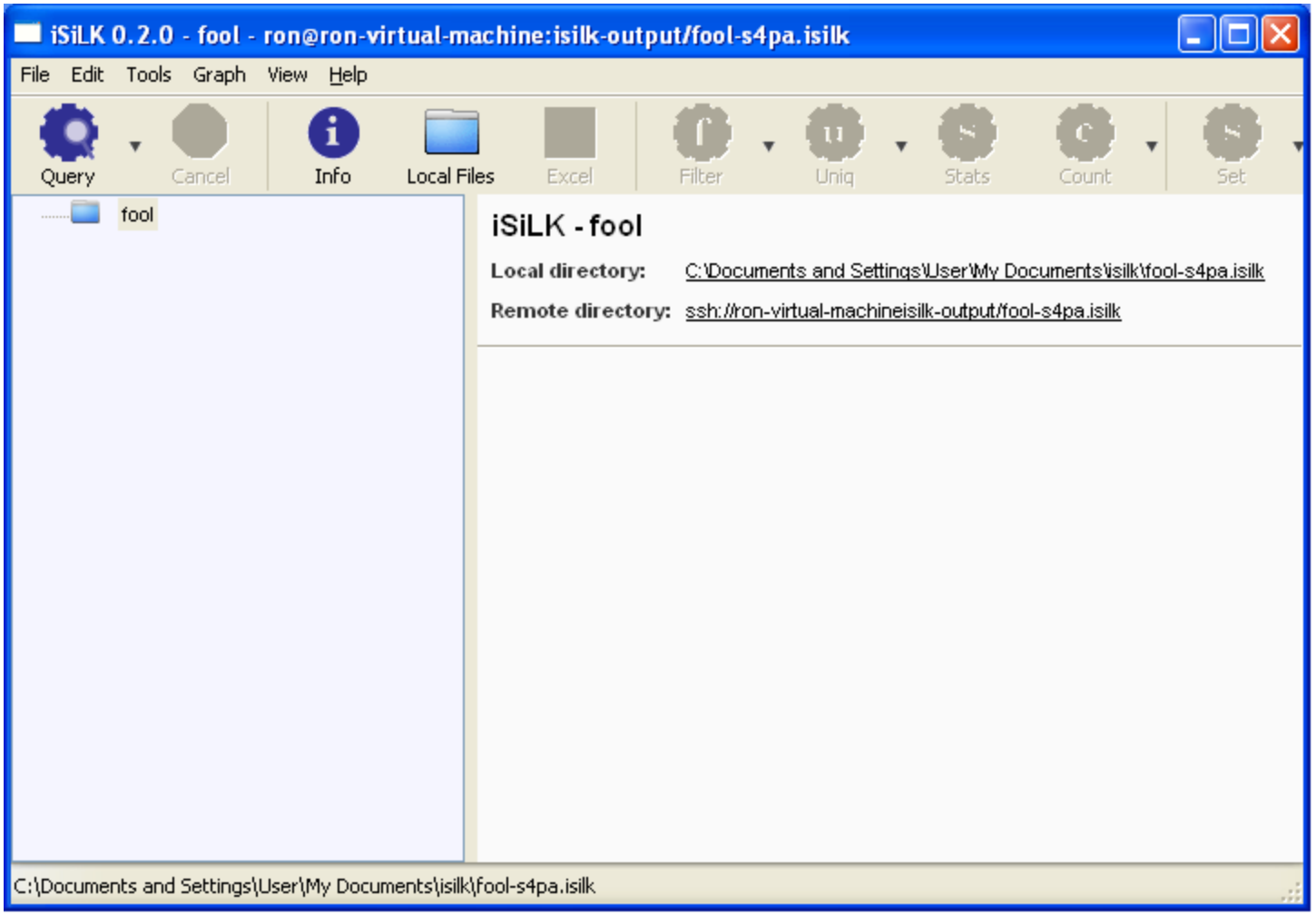
iSiLK Configuration:

Remote_Host:	localhost (default)
Remote_Port:	22 (default)
Remote_User:	**liveuser**
RSH_Key:	**/home/liveuser/.ssh/id_rsa**
Rmt_Output:	**isilk-output**
Rmt_Library:	**isilk-libs**

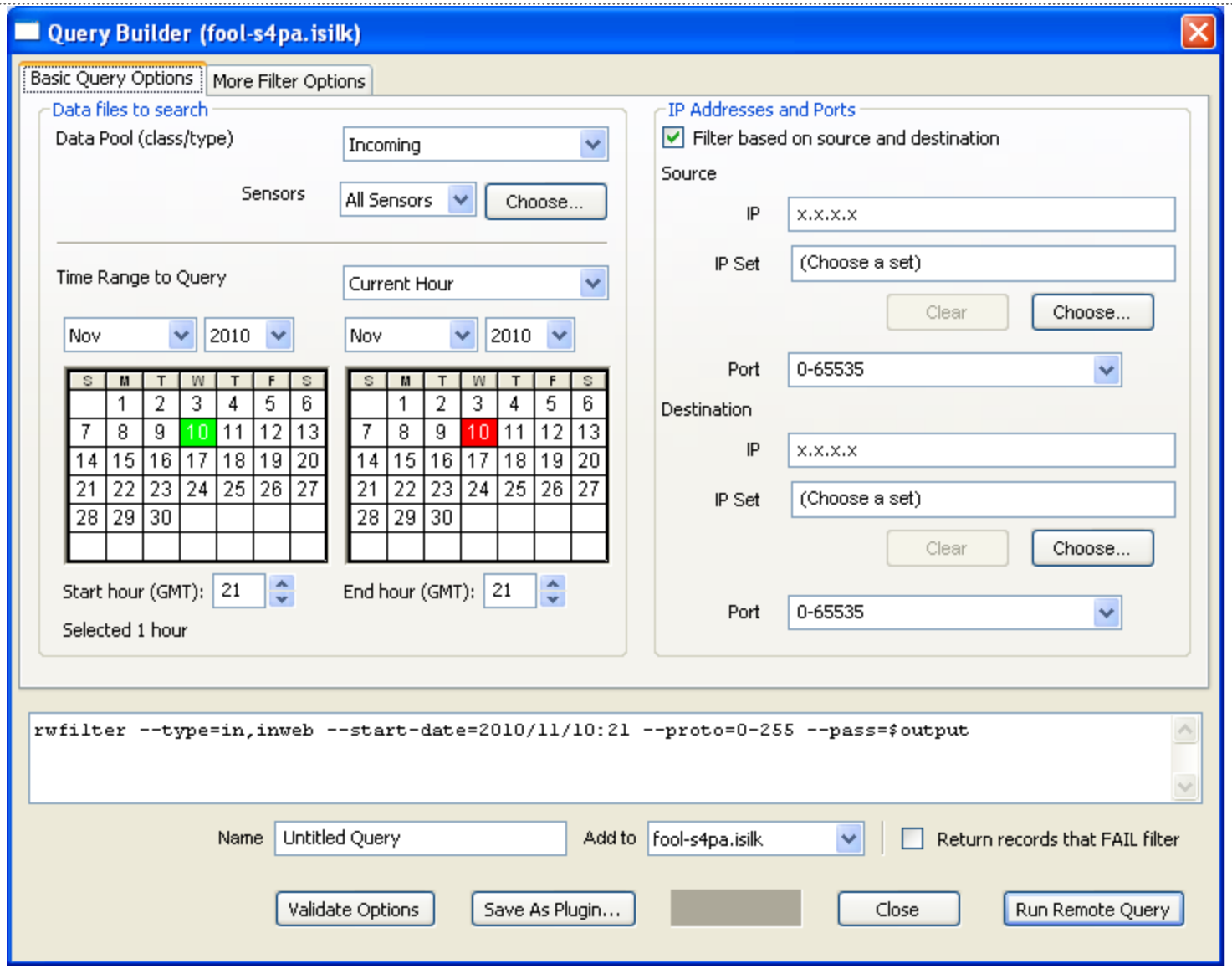
First Screen — Problem Sets



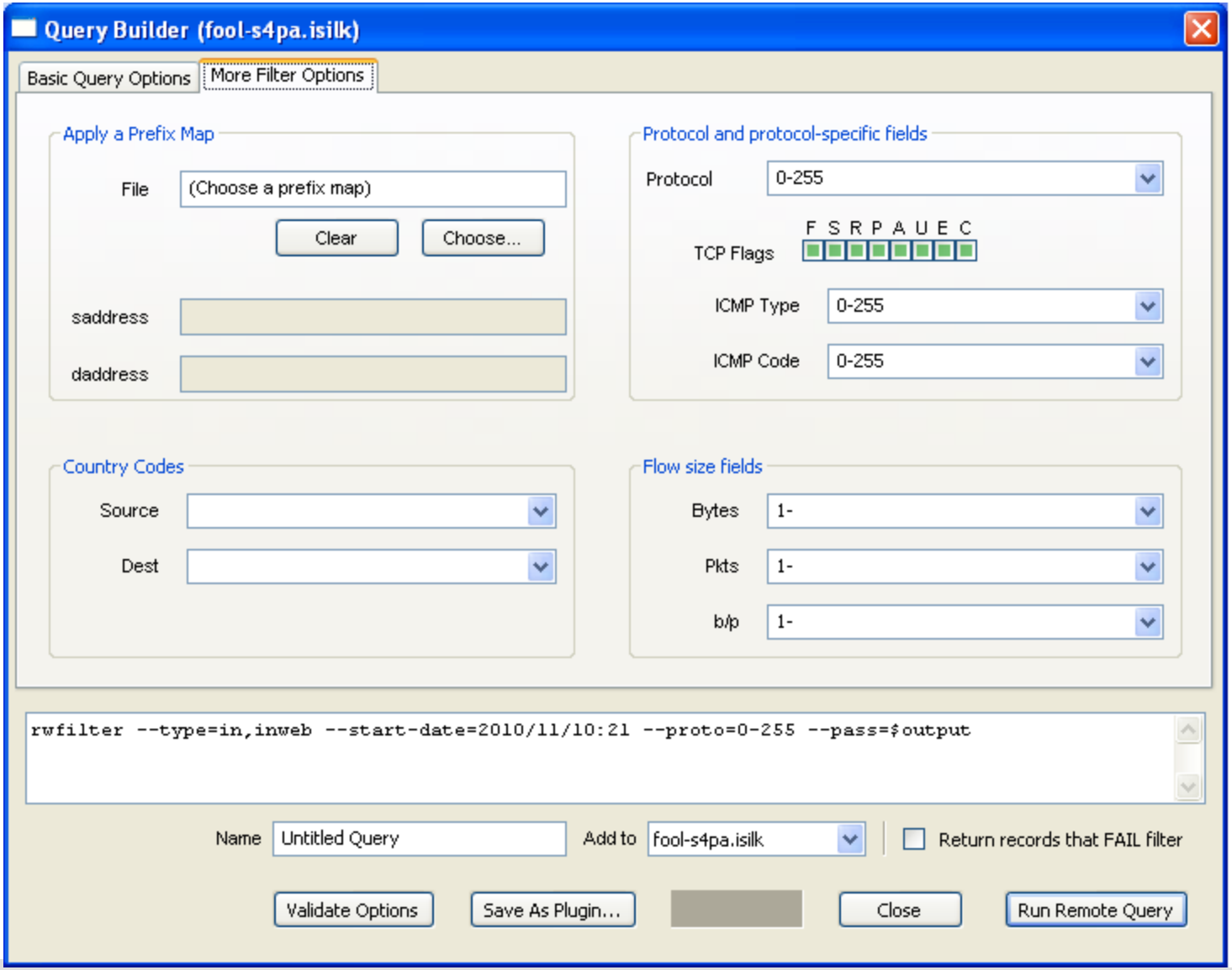
Main Screen


iSiLK 0.2.0 - fool - ron@ron-virtual-machine:isilk-output/fool-s4pa.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
fool
iSiLK - fool
Local directory: C:\Documents and Settings\User\My Documents\isilk\fool-s4pa.isilk
Remote directory: ssh://ron-virtual-machineisilk-output/fool-s4pa.isilk
C:\Documents and Settings\User\My Documents\isilk\fool-s4pa.isilk

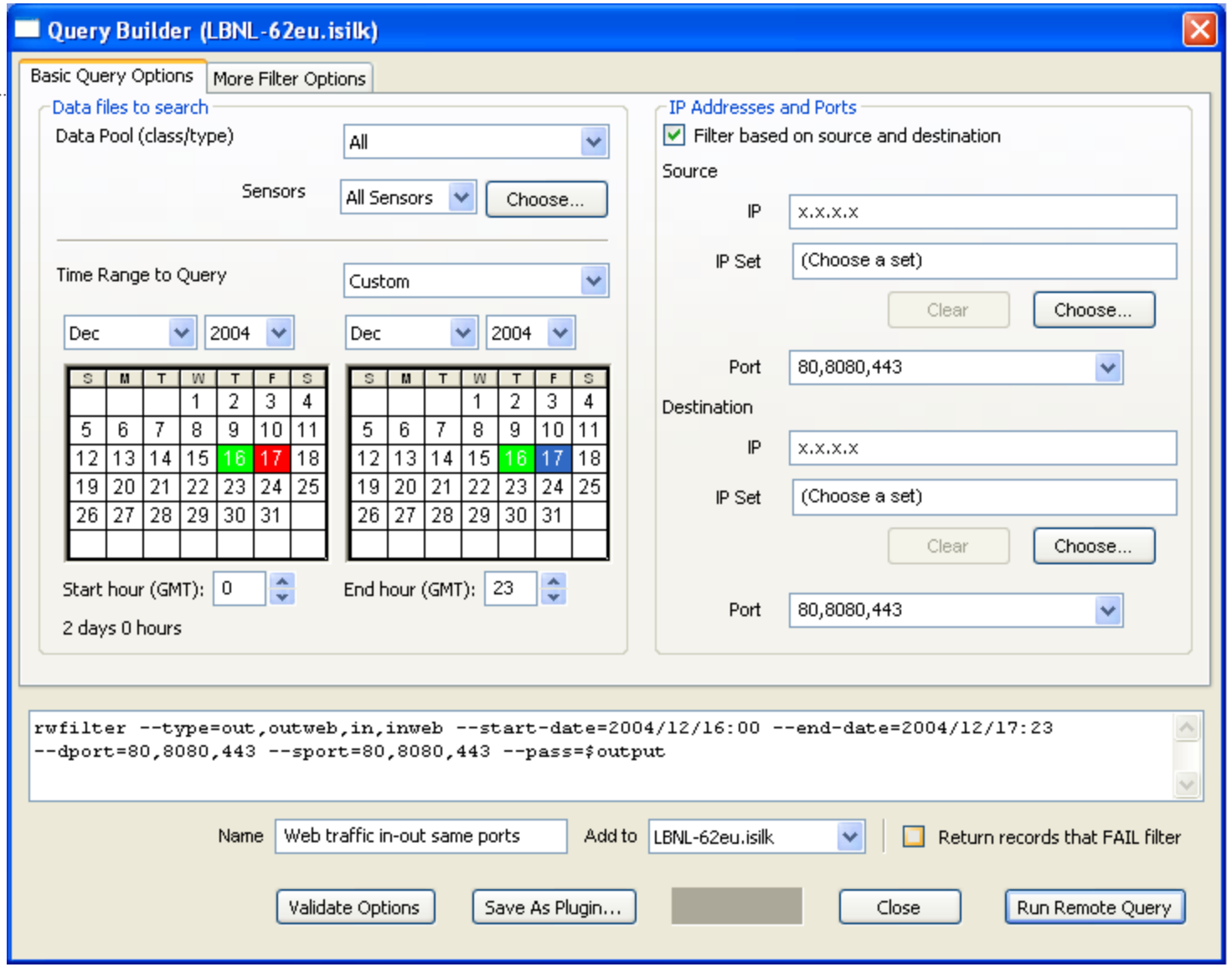
Query Builder

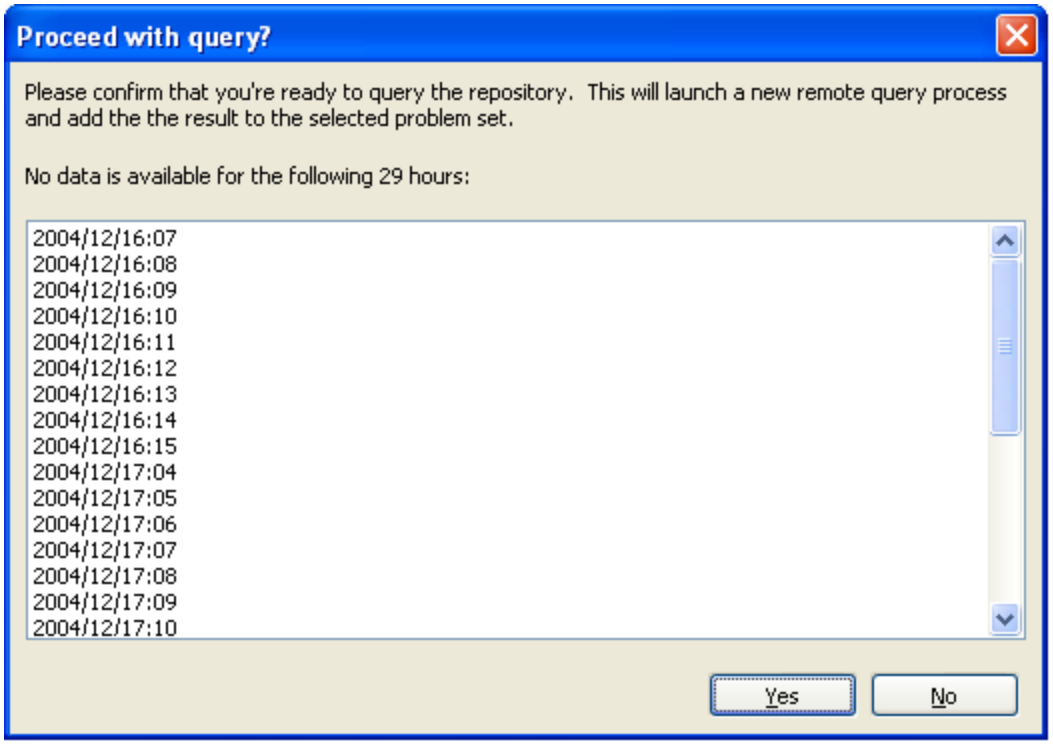


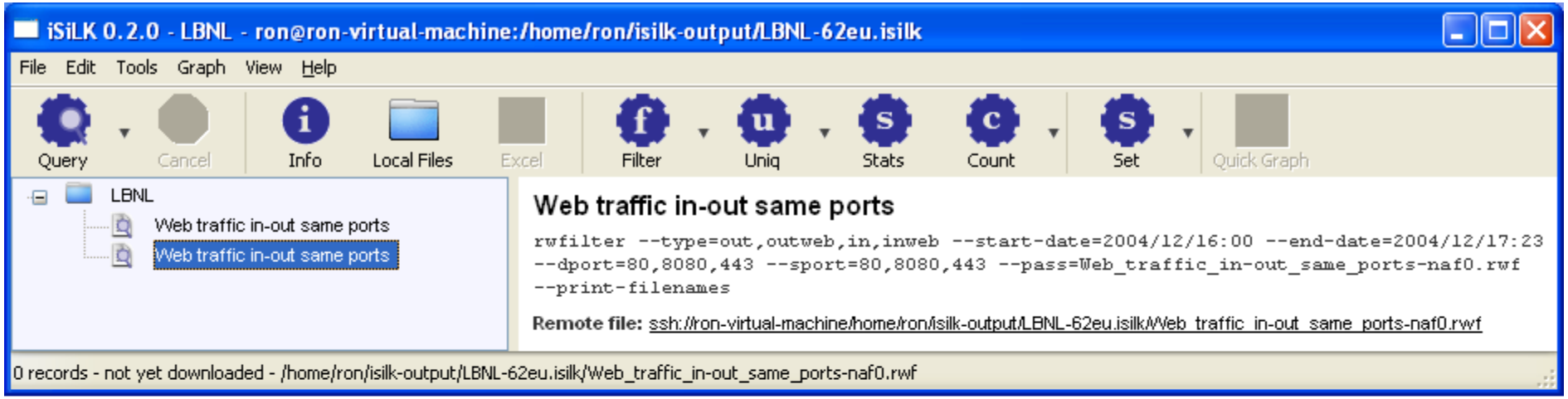
Query Builder—more filter options

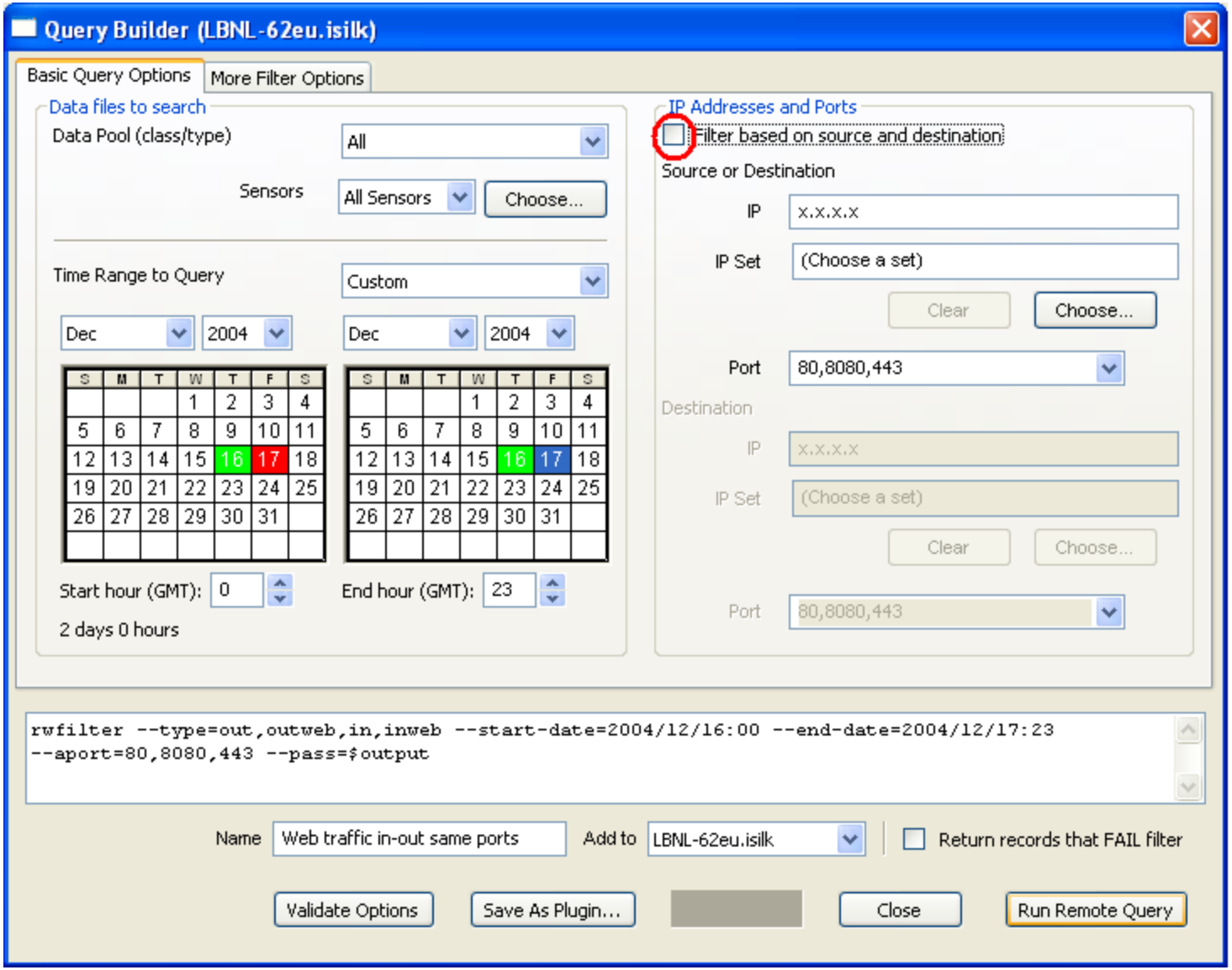


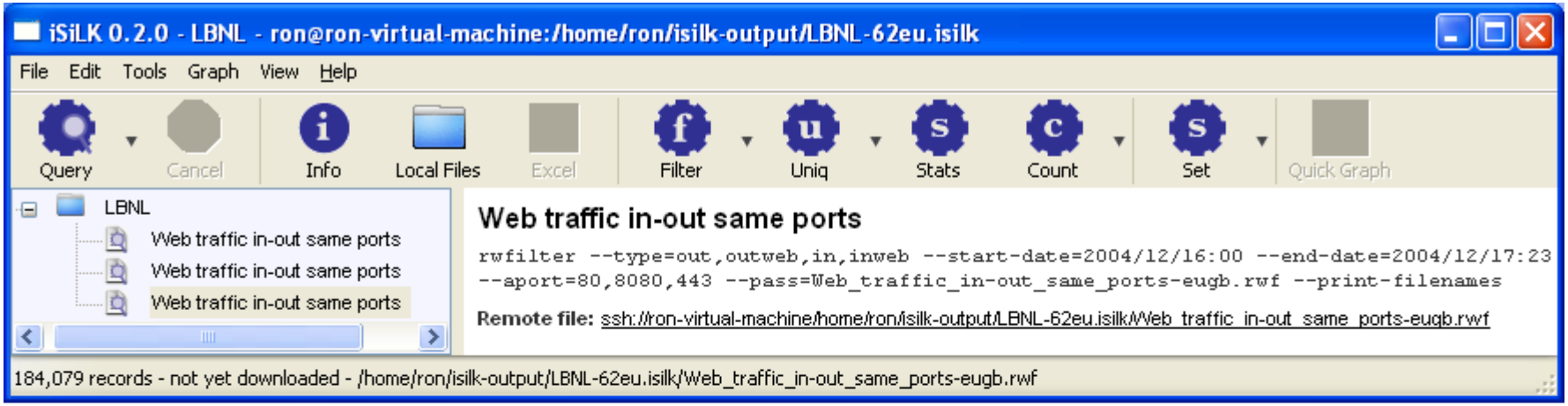
Demonstration

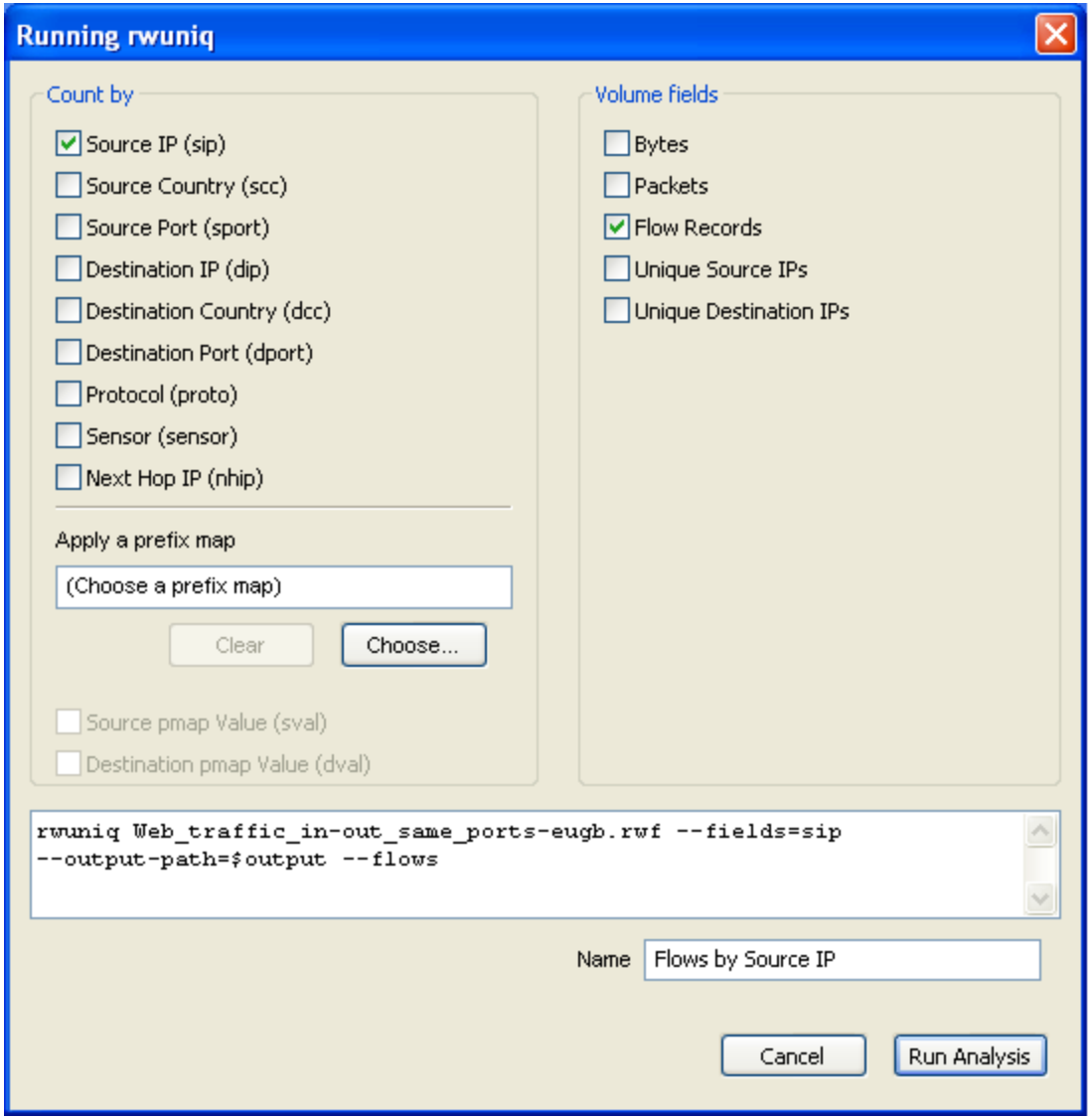

Query Builder (LBNL-62eu.isilk)
Basic Query Options
More Filter Options
Data files to search
Data Pool (class/type)
All
Sensors
All Sensors
Choose...
Time Range to Query
Custom
Dec
2004
Dec
2004
S M T W T F S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
Start hour (GMT): 0
End hour (GMT): 23
2 days 0 hours
IP Addresses and Ports
Filter based on source and destination
Source
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
80,8080,443
Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
80,8080,443
rwfilter --type=out,outweb,in,inweb --start-date=2004/12/16:00 --end-date=2004/12/17:23
--dport=80,8080,443 --sport=80,8080,443 --pass=$output
Name
Web traffic in-out same ports
Add to
LBNL-62eu.isilk
Return records that FAIL filter
Validate Options
Save As Plugin...
Close
Run Remote Query

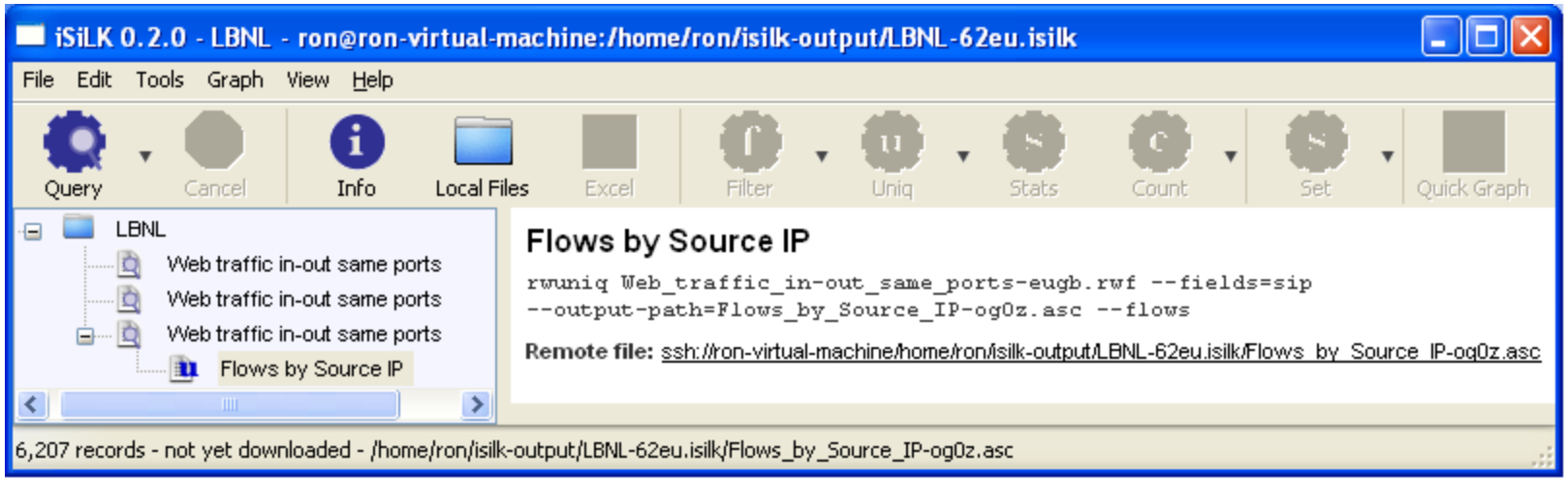

Proceed with query?
Please confirm that you're ready to query the repository. This will launch a new remote query process and add the the result to the selected problem set.
No data is available for the following 29 hours:
2004/12/16:07
2004/12/16:08
2004/12/16:09
2004/12/16:10
2004/12/16:11
2004/12/16:12
2004/12/16:13
2004/12/16:14
2004/12/16:15
2004/12/17:04
2004/12/17:05
2004/12/17:06
2004/12/17:07
2004/12/17:08
2004/12/17:09
2004/12/17:10
Yes
No

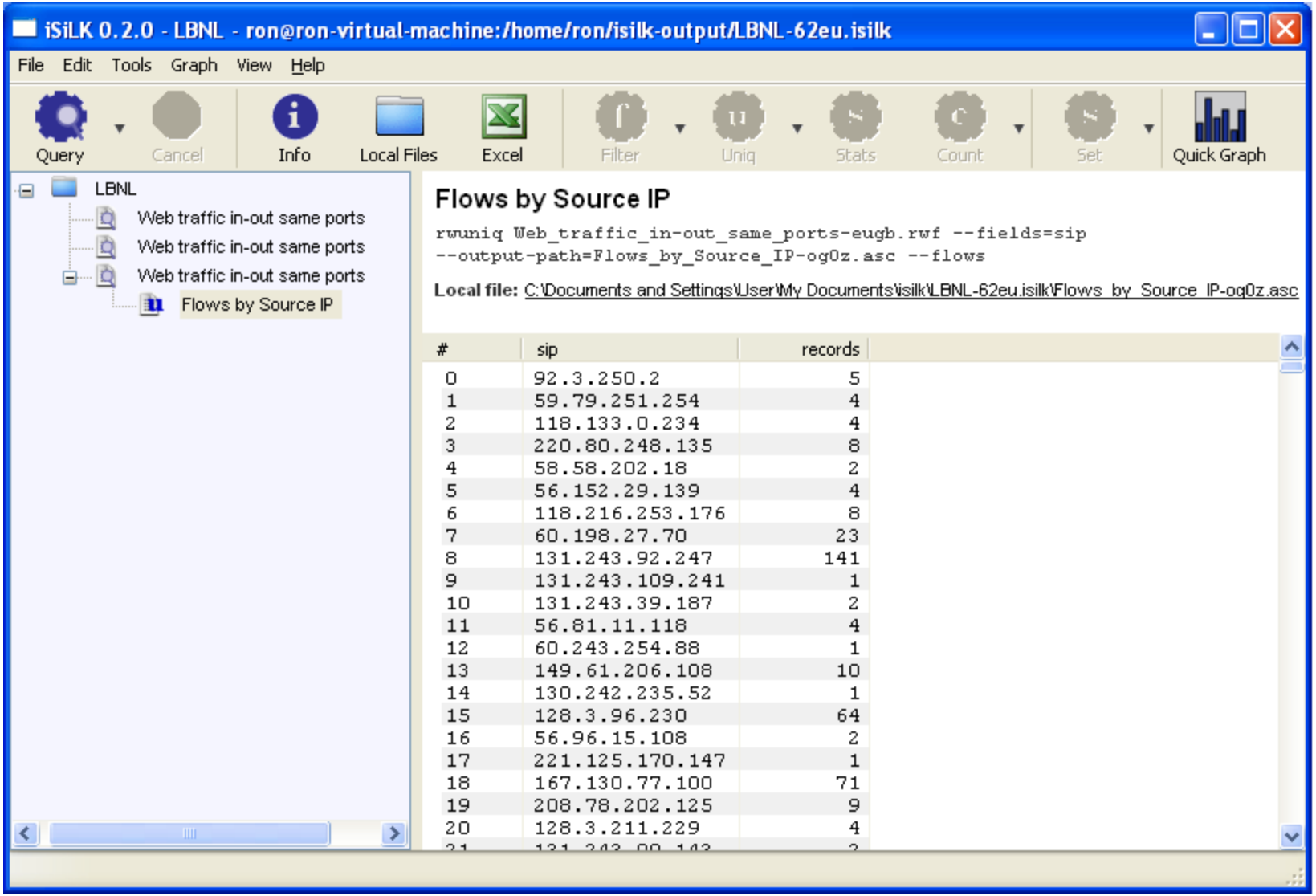

iSiLK 0.2.0 - LBNL - ron@ron-virtual-machine:/home/ron/isilk-output/LBNL-62eu.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
LBNL
Web traffic in-out same ports
Web traffic in-out same ports
Web traffic in-out same ports
rwfilter --type=out,outweb,in,inweb --start-date=2004/12/16:00 --end-date=2004/12/17:23
--dport=80,8080,443 --sport=80,8080,443 --pass=Web_traffic_in-out_same_ports-naf0.rwf
--print-filenames
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/LBNL-62eu.isilk/Web_traffic_in-out_same_ports-naf0.rwf
0 records - not yet downloaded - /home/ron/isilk-output/LBNL-62eu.isilk/Web_traffic_in-out_same_ports-naf0.rwf

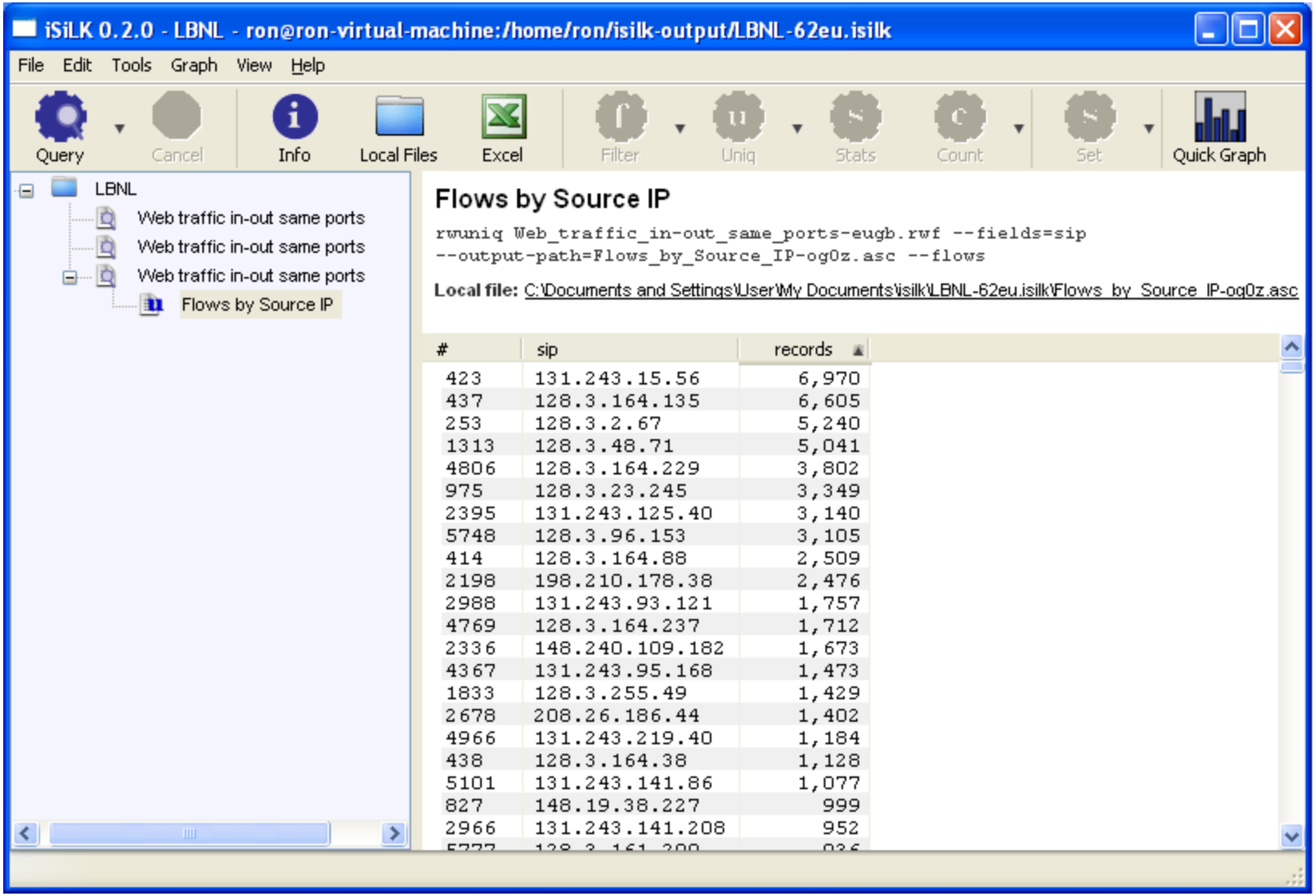

Query Builder (LBNL-62eu.isilk)
Basic Query Options
More Filter Options
Data files to search
Data Pool (class/type)
All
Sensors
All Sensors
Choose...
Time Range to Query
Custom
Dec
2004
Dec
2004
S M T W T F S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
Start hour (GMT): 0
End hour (GMT): 23
2 days 0 hours
IP Addresses and Ports
Filter based on source and destination
Source or Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
80,8080,443
Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
80,8080,443
rwfilter --type=out,outweb,in,inweb --start-date=2004/12/16:00 --end-date=2004/12/17:23
--aport=80,8080,443 --pass=$output
Name
Web traffic in-out same ports
Add to
LBNL-62eu.isilk
Return records that FAIL filter
Validate Options
Save As Plugin...
Close
Run Remote Query

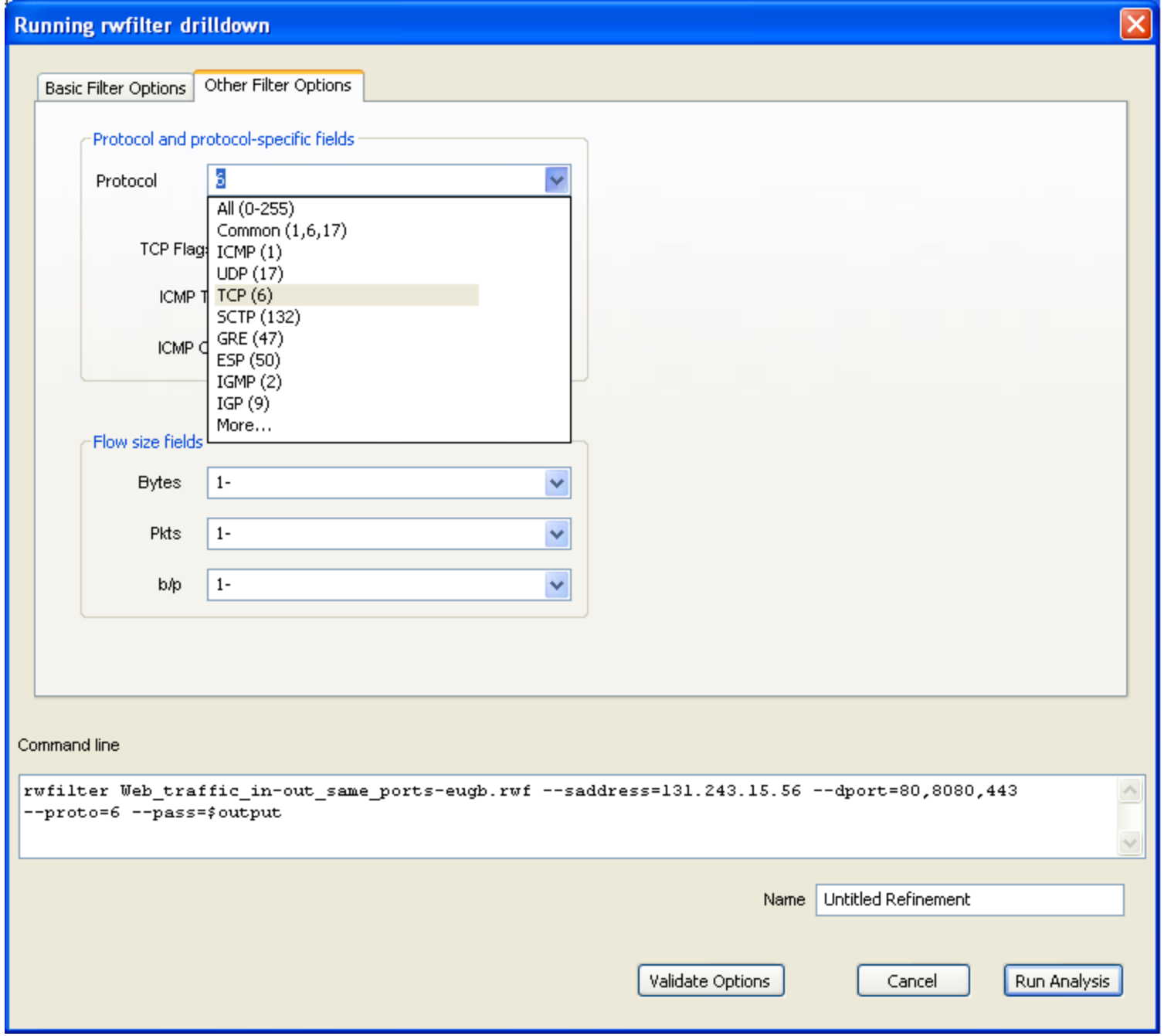

iSiLK 0.2.0 - LBNL - ron@ron-virtual-machine:/home/ron/isilk-output/LBNL-62eu.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
LBNL
Web traffic in-out same ports
Web traffic in-out same ports
Web traffic in-out same ports
Web traffic in-out same ports
rwfilter --type=out,outweb,in,inweb --start-date=2004/12/16:00 --end-date=2004/12/17:23
--aport=80,8080,443 --pass=Web_traffic_in-out_same_ports-eugb.rwf --print-filenames
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/LBNL-62eu.isilk/Web_traffic_in-out_same_ports-eugb.rwf
184,079 records - not yet downloaded - /home/ron/isilk-output/LBNL-62eu.isilk/Web_traffic_in-out_same_ports-eugb.rwf

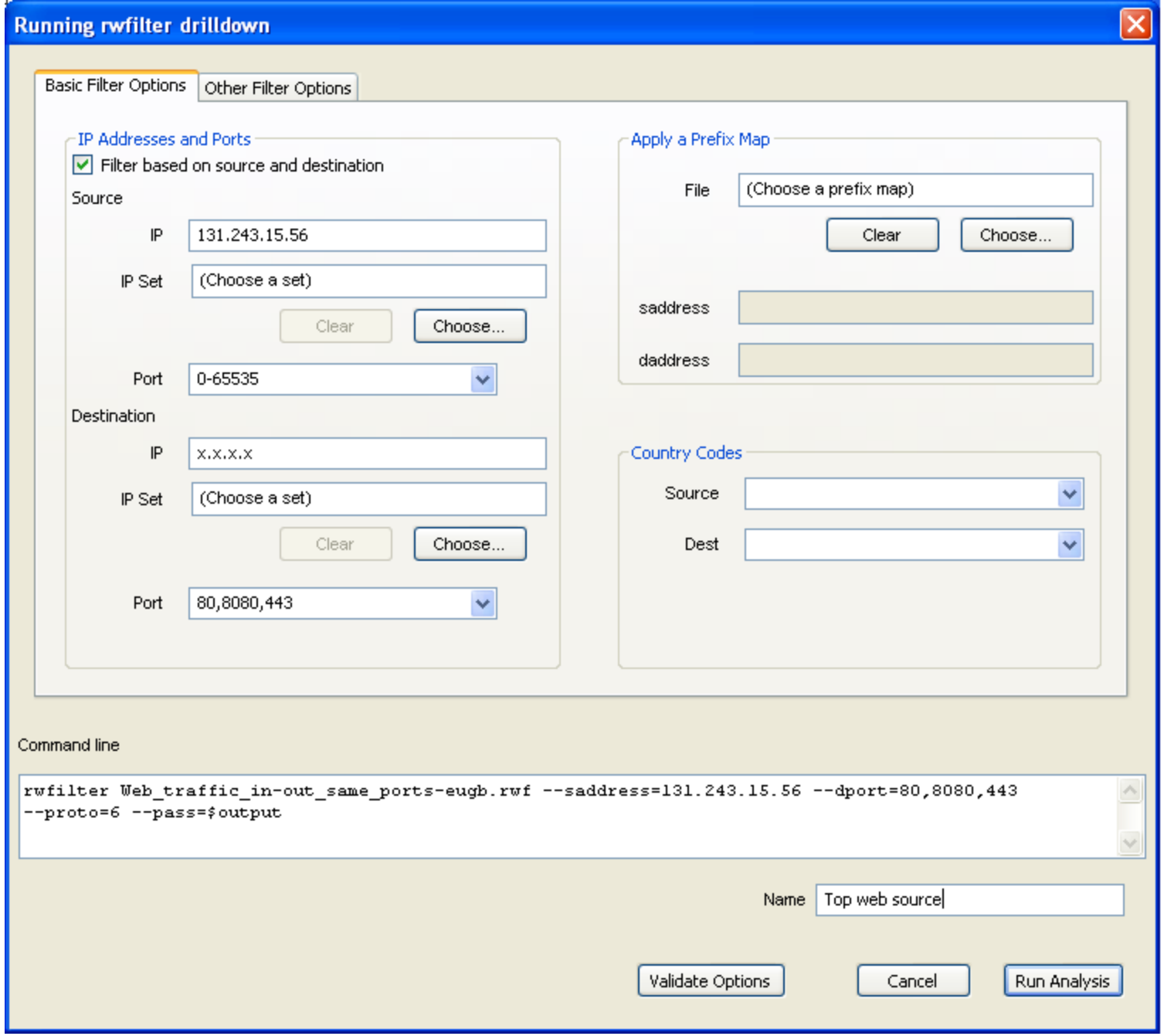

Running rwuniq
Count by
Source IP (sip)
Source Country (scc)
Source Port (sport)
Destination IP (dip)
Destination Country (dcc)
Destination Port (dport)
Protocol (proto)
Sensor (sensor)
Next Hop IP (nhip)
Apply a prefix map
(Choose a prefix map)
Clear
Choose...
Source pmap Value (sval)
Destination pmap Value (dval)
Volume fields
Bytes
Packets
Flow Records
Unique Source IPs
Unique Destination IPs
rwuniq Web_traffic_in-out_same_ports-eugb.rwf --fields=sip
--output-path=$output --flows
Name
Flows by Source IP
Cancel
Run Analysis

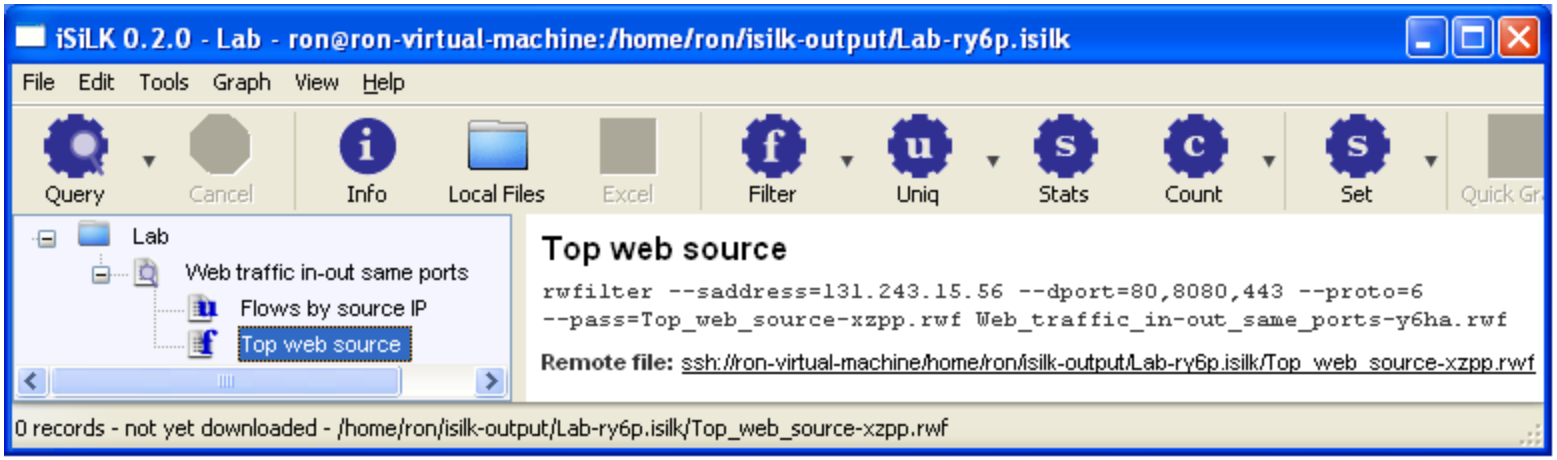

iSiLK 0.2.0 - LBNL - ron@ron-virtual-machine:/home/ron/isilk-output/LBNL-62eu.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
LBNL
Web traffic in-out same ports
Web traffic in-out same ports
Web traffic in-out same ports
Flows by Source IP
Flows by Source IP
rwuniq Web_traffic_in-out_same_ports-eugb.rwf --fields=sip
--output-path=Flows_by_Source_IP-og0z.asc --flows
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/LBNL-62eu.isilk/Flows_by_Source_IP-og0z.asc
6,207 records - not yet downloaded - /home/ron/isilk-output/LBNL-62eu.isilk/Flows_by_Source_IP-og0z.asc

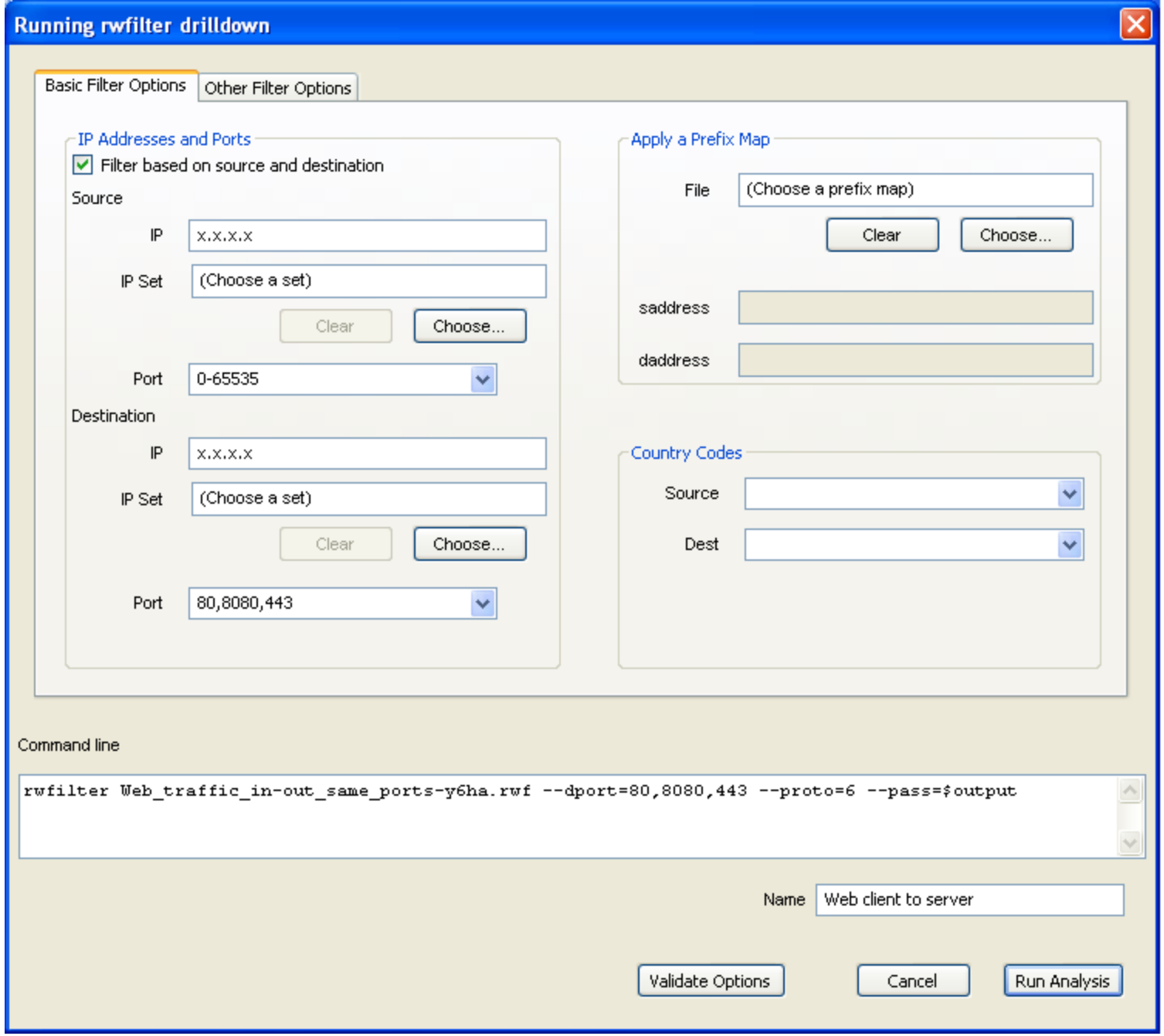

iSiLK 0.2.0 - LBNL - ron@ron-virtual-machine:/home/ron/isilk-output/LBNL-62eu.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
LBNL
Web traffic in-out same ports
Web traffic in-out same ports
Web traffic in-out same ports
Flows by Source IP
Flows by Source IP
rwuniq Web_traffic_in-out_same_ports-eugb.rwf --fields=sip
--output-path=Flows_by_Source_IP-og0z.asc --flows
Local file: C:\Documents and Settings\User\My Documents\isilk\LBNL-62eu.isilk\Flows_by_Source_IP-og0z.asc
sip records
0 92.3.250.2 5
1 59.79.251.254 4
2 118.133.0.234 4
3 220.80.248.135 8
4 58.58.202.18 2
5 56.152.29.139 4
6 118.216.253.176 8
7 60.198.27.70 23
8 131.243.92.247 141
9 131.243.109.241 1
10 131.243.39.187 2
11 56.81.11.118 4
12 60.243.254.88 1
13 149.61.206.108 10
14 130.242.235.52 1
15 128.3.96.230 64
16 56.96.15.108 2
17 221.125.170.147 1
18 167.130.77.100 71
19 208.78.202.125 9
20 128.3.211.229 4

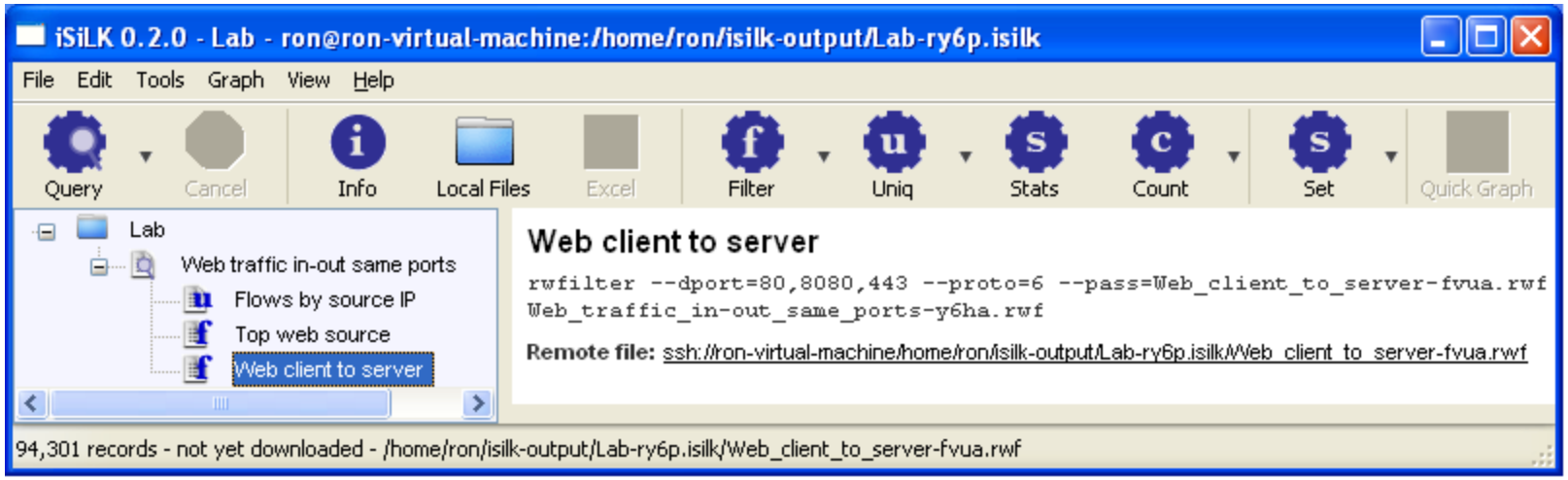

iSiLK 0.2.0 - LBNL - ron@ron-virtual-machine:/home/ron/isilk-output/LBNL-62eu.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
LBNL
Web traffic in-out same ports
Web traffic in-out same ports
Web traffic in-out same ports
Flows by Source IP
Flows by Source IP
rwuniq Web_traffic_in-out_same_ports-eugb.rwf --fields=sip
--output-path=Flows_by_Source_IP-og0z.asc --flows
Local file: C:\Documents and Settings\User\My Documents\isilk\LBNL-62eu.isilk\Flows_by_Source_IP-og0z.asc
sip records
423 131.243.15.56 6,970
437 128.3.164.135 6,605
253 128.3.2.67 5,240
1313 128.3.48.71 5,041
4806 128.3.164.229 3,802
975 128.3.23.245 3,349
2395 131.243.125.40 3,140
5748 128.3.96.153 3,105
414 128.3.164.88 2,509
2198 198.210.178.38 2,476
2988 131.243.93.121 1,757
4769 128.3.164.237 1,712
2336 148.240.109.182 1,673
4367 131.243.95.168 1,473
1833 128.3.255.49 1,429
2678 208.26.186.44 1,402
4966 131.243.219.40 1,184
438 128.3.164.38 1,128
5101 131.243.141.86 1,077
827 148.19.38.227 999
2966 131.243.141.208 952

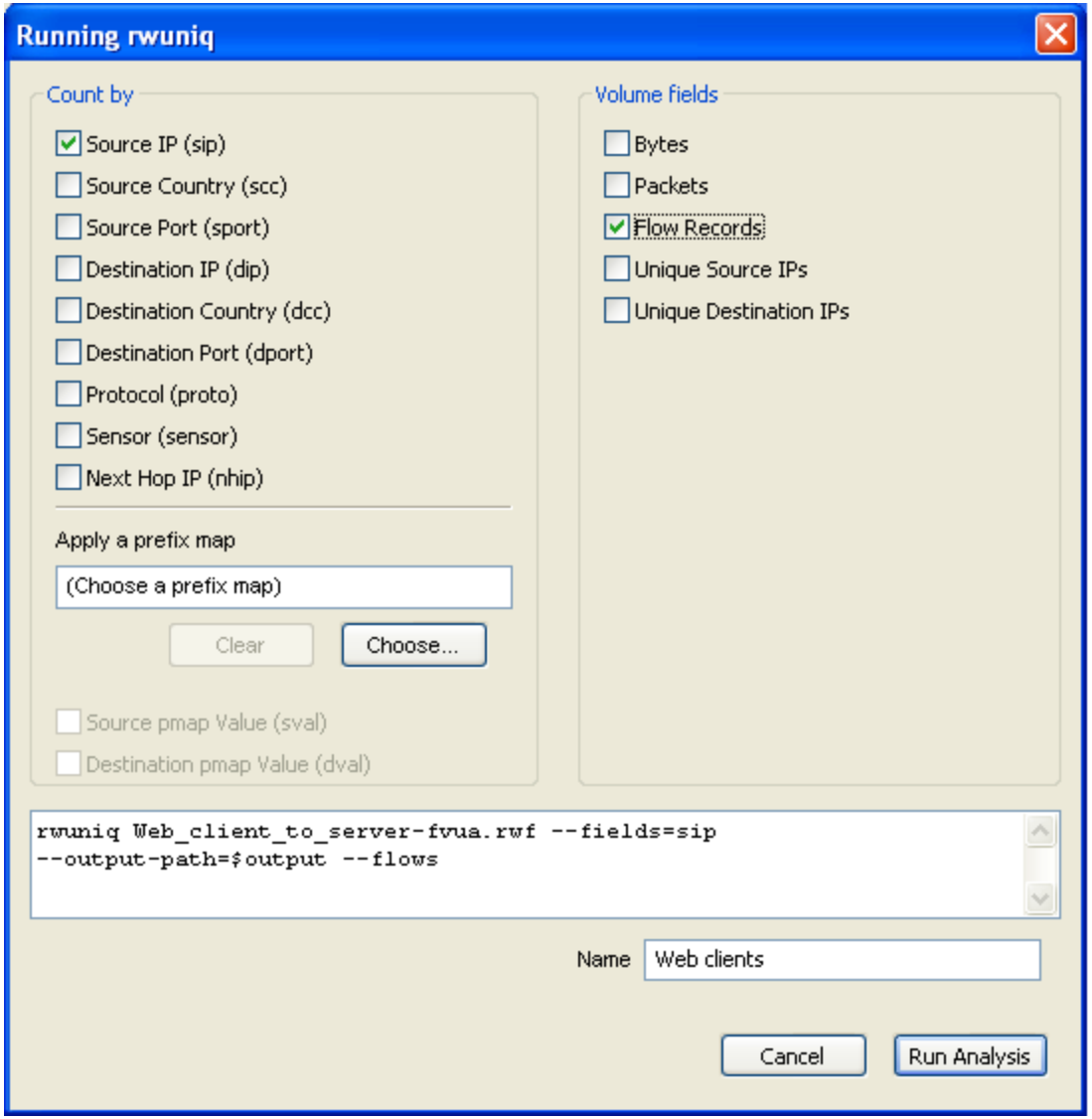

Running rwfilter drilldown
Basic Filter Options
Other Filter Options
Protocol and protocol-specific fields
Protocol
3
All (0-255)
Common (1,6,17)
ICMP (1)
UDP (17)
TCP (6)
SCTP (132)
GRE (47)
ESP (50)
IGMP (2)
IGP (9)
More...
Flow size fields
Bytes
1-
Pkts
1-
b/p
1-
Command line
rwfilter Web_traffic_in-out_same_ports-eugb.rwf --saddress=131.243.15.56 --dport=80,8080,443
--proto=6 --pass=$output
Name
Untitled Refinement
Validate Options
Cancel
Run Analysis

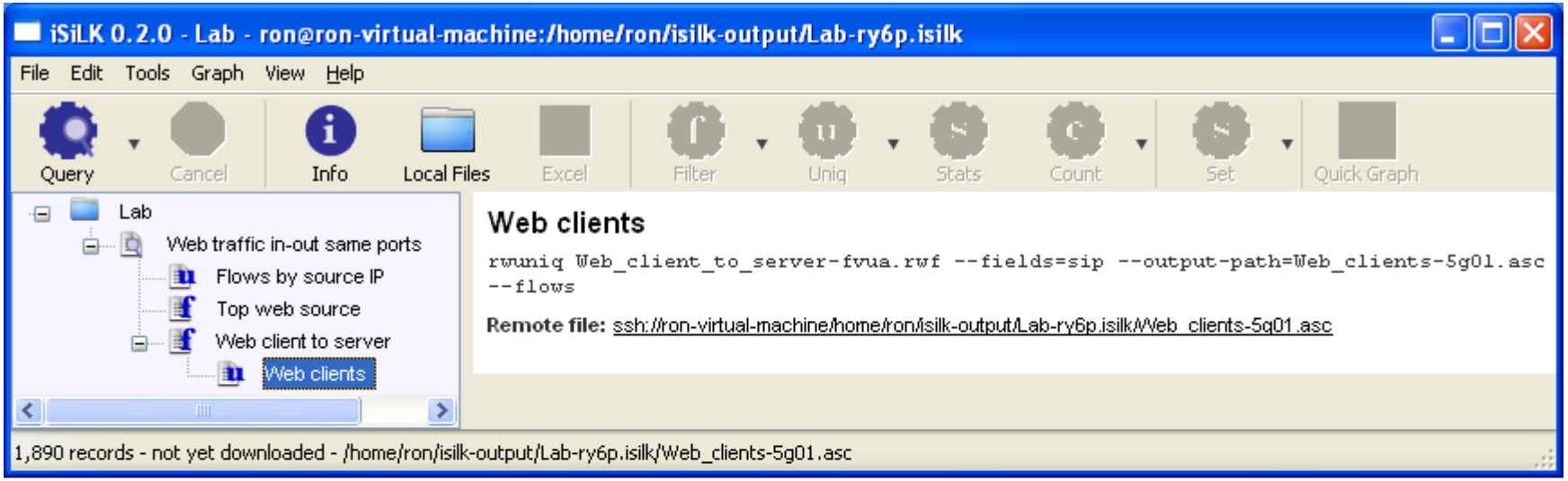

Running rwfilter drilldown
Basic Filter Options
Other Filter Options
IP Addresses and Ports
Filter based on source and destination
Source
IP
131.243.15.56
IP Set
(Choose a set)
Clear
Choose...
Port
0-65535
Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
80,8080,443
Apply a Prefix Map
File
(Choose a prefix map)
Clear
Choose...
saddress
daddress
Country Codes
Source
Dest
Command line
rwfilter Web_traffic_in-out_same_ports-eugb.rwf --saddress=131.243.15.56 --dport=80,8080,443
--proto=6 --pass=$output
Name
Top web source
Validate Options
Cancel
Run Analysis

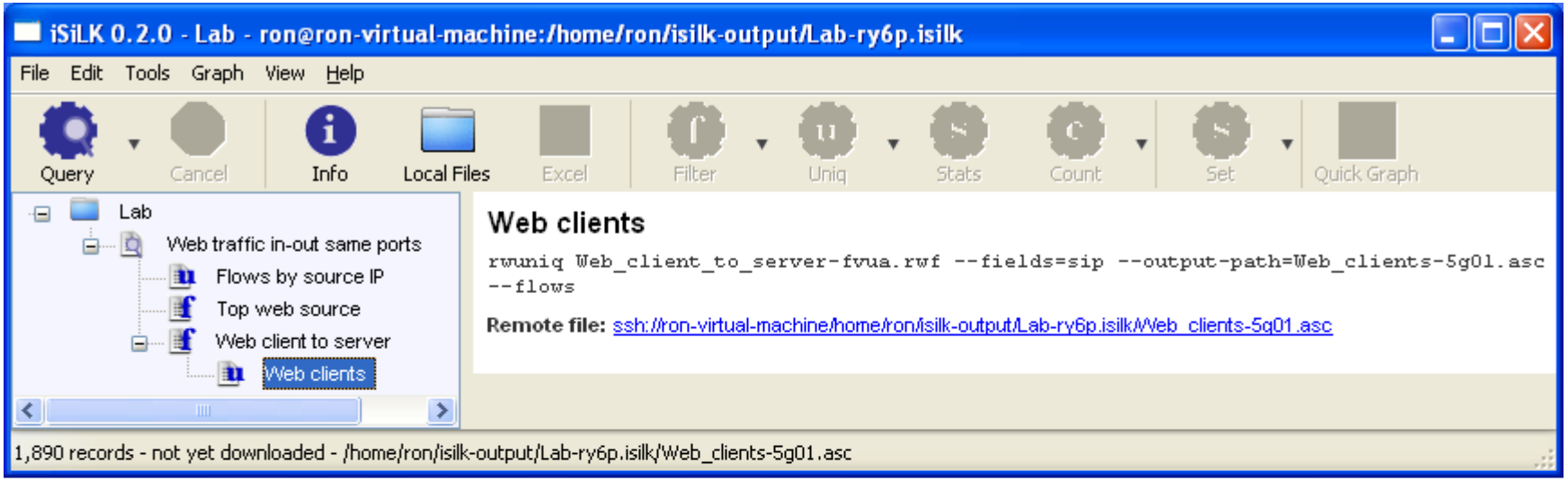

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Top web source
rwfilter --saddress=131.243.15.56 --dport=80,8080,443 --proto=6
--pass=Top_web_source-xzpp.rwf Web_traffic_in-out_same_ports-y6ha.rwf
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_web_source-xzpp.rwf
0 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Top_web_source-xzpp.rwf

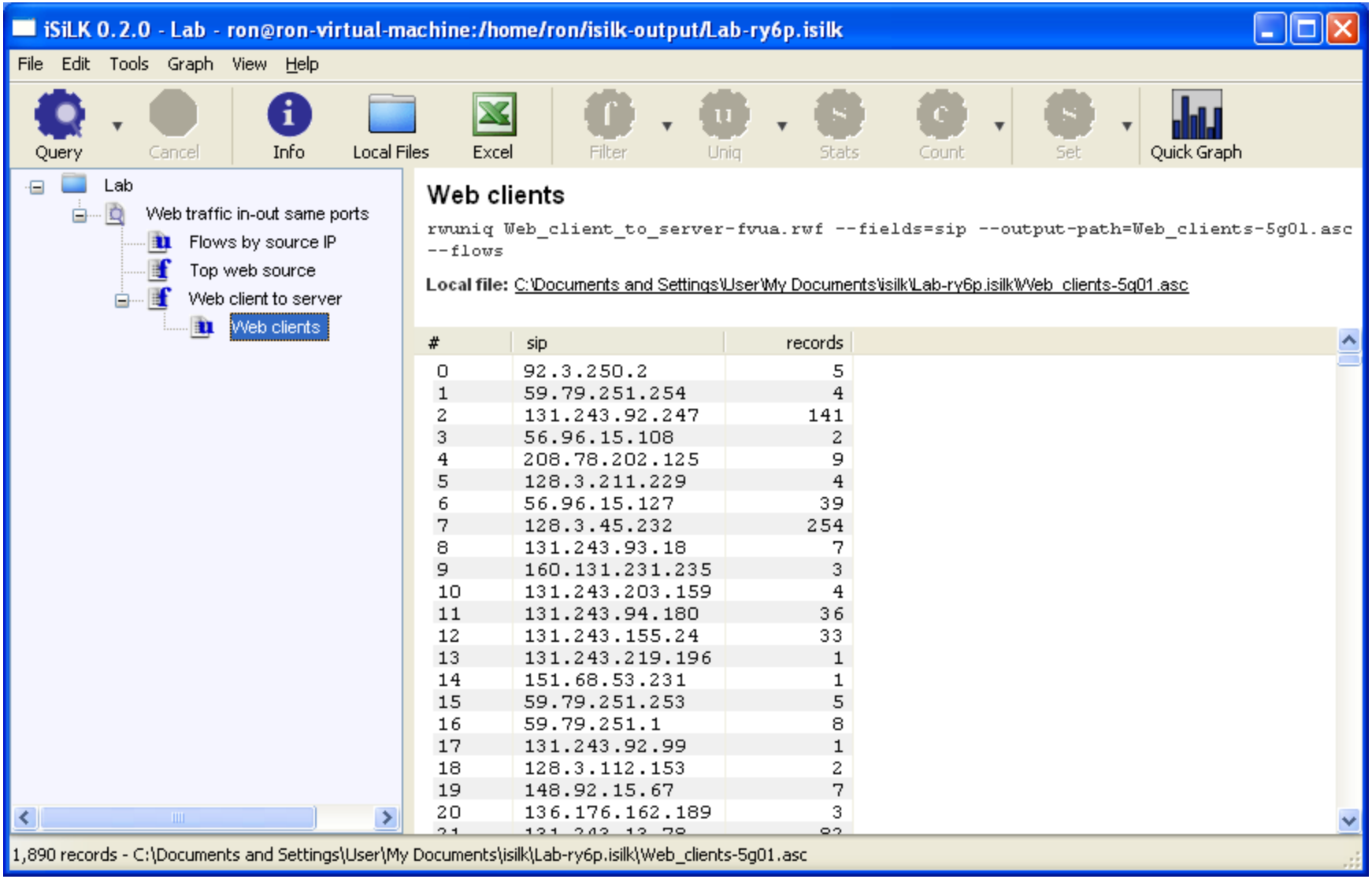

Running rwfilter drilldown
Basic Filter Options
Other Filter Options
IP Addresses and Ports
Filter based on source and destination
Source
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
0-65535
Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
80,8080,443
Apply a Prefix Map
File
(Choose a prefix map)
Clear
Choose...
saddress
daddress
Country Codes
Source
Dest
Command line
rwfilter Web_traffic_in-out_same_ports-y6ha.rwf --dport=80,8080,443 --proto=6 --pass=$output
Name
Web client to server
Validate Options
Cancel
Run Analysis

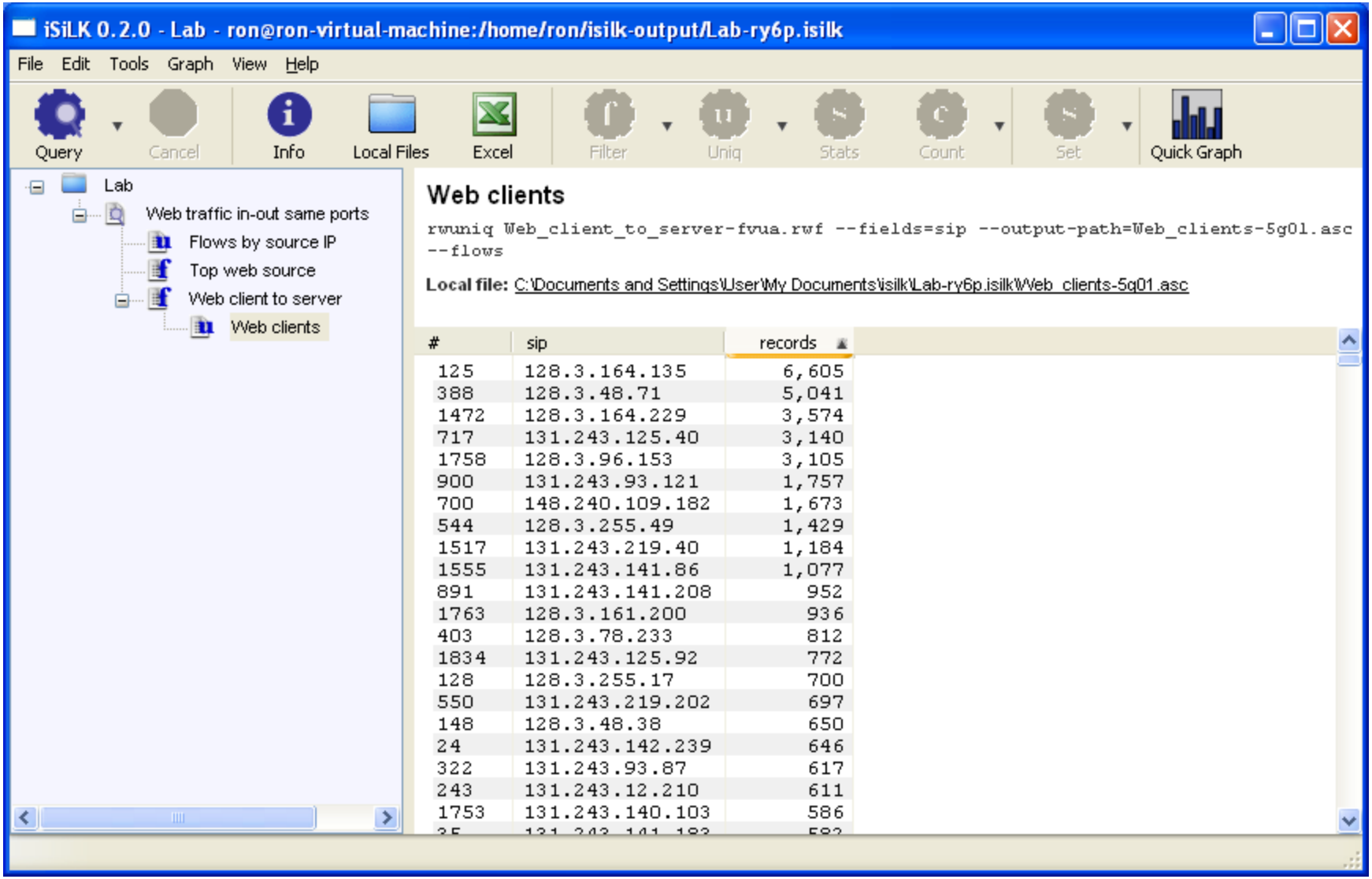

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web client to server
rwfilter --dport=80,8080,443 --proto=6 --pass=Web_client_to_server-fvua.rwf Web_traffic_in-out_same_ports-y6ha.rwf
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Web_client_to_server-fvua.rwf
94,301 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Web_client_to_server-fvua.rwf

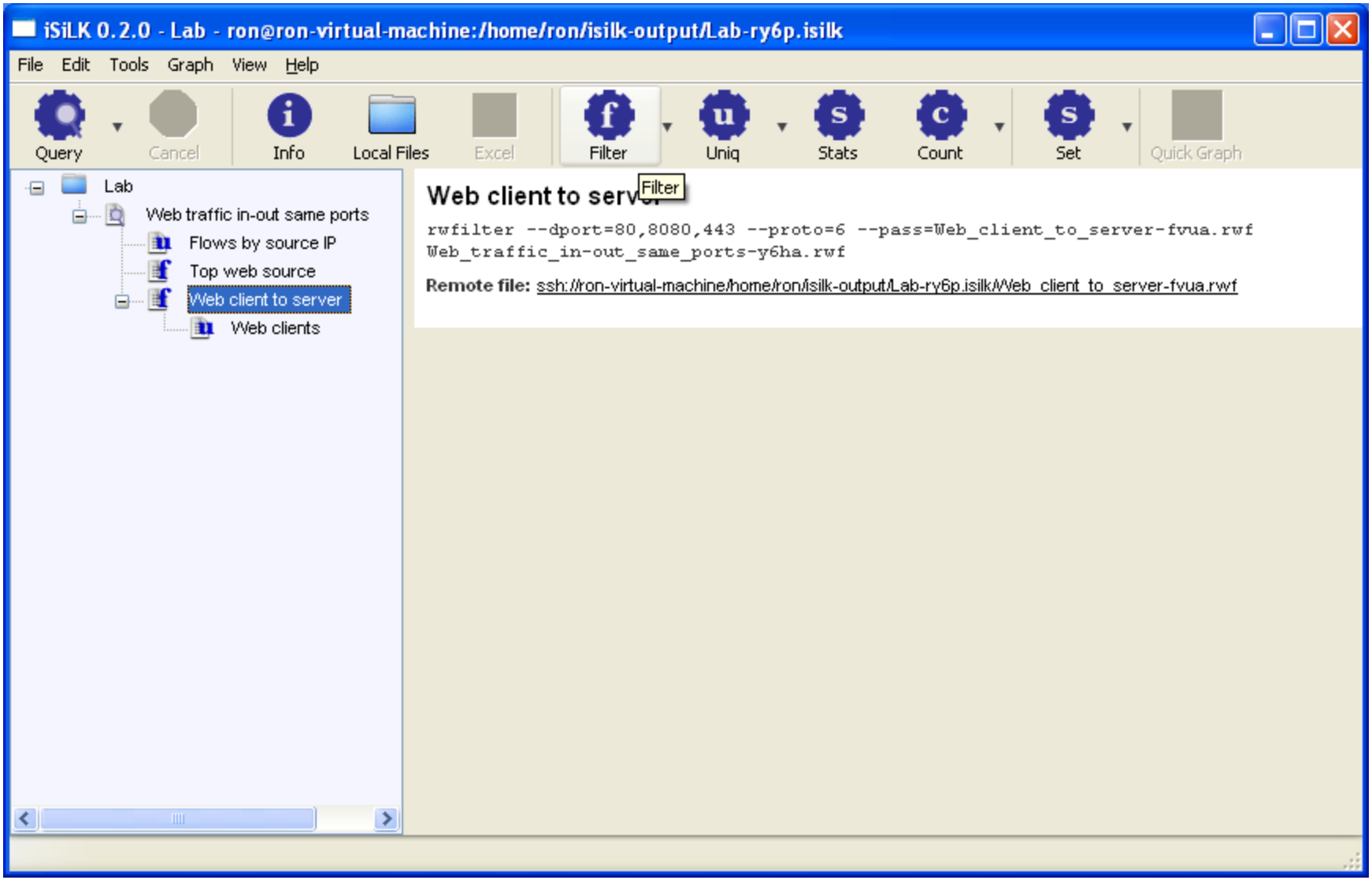

Running rwuniq
Count by
Source IP (sip)
Source Country (scc)
Source Port (sport)
Destination IP (dip)
Destination Country (dcc)
Destination Port (dport)
Protocol (proto)
Sensor (sensor)
Next Hop IP (nhip)
Apply a prefix map
(Choose a prefix map)
Clear
Choose...
Source pmap Value (sval)
Destination pmap Value (dval)
Volume fields
Bytes
Packets
Flow Records
Unique Source IPs
Unique Destination IPs
rwuniq Web_client_to_server-fvua.rwf --fields=sip
--output-path=$output --flows
Name
Web clients
Cancel
Run Analysis

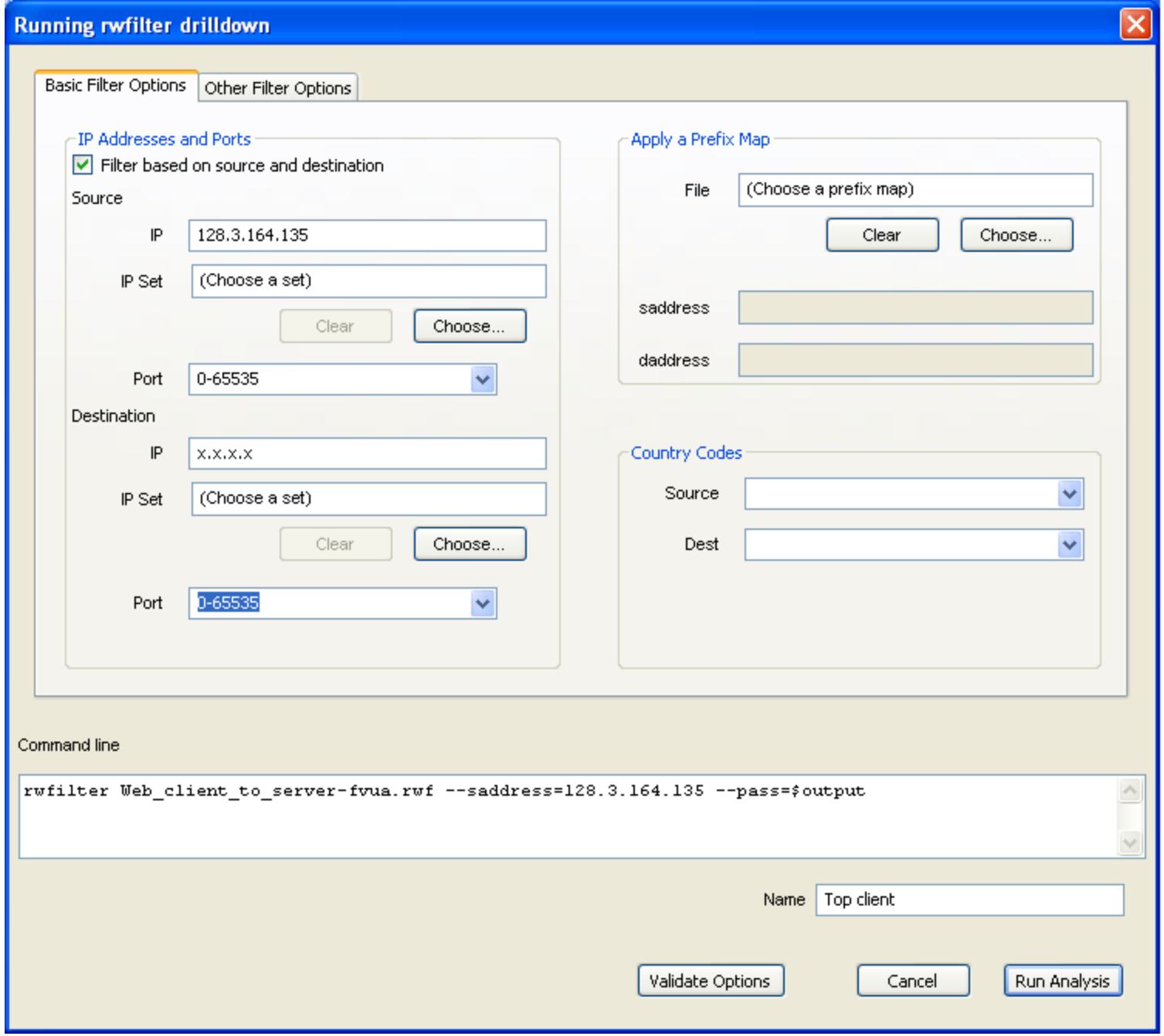

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Web clients
rwuniq Web_client_to_server-fvua.rwf --fields=sip --output-path=Web_clients-5g01.asc --flows
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Web_clients-5g01.asc
1,890 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Web_clients-5g01.asc

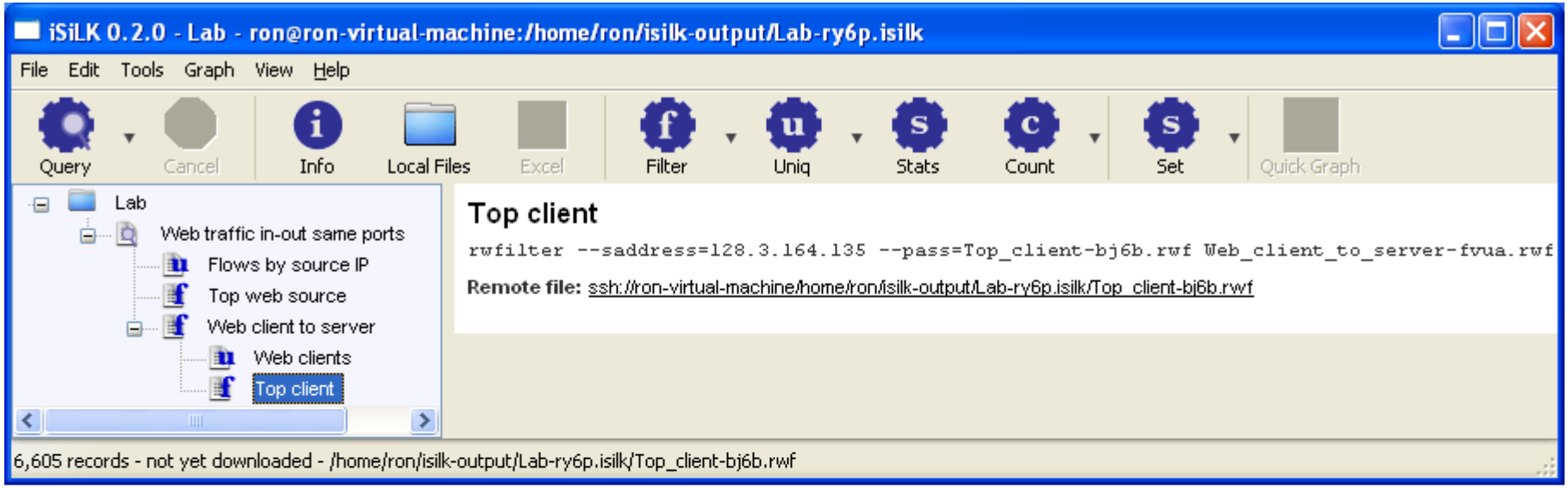

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Web clients
rwuniq Web_client_to_server-fvua.rwf --fields=sip --output-path=Web_clients-5g01.asc --flows
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Web_clients-5g01.asc
1,890 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Web_clients-5g01.asc

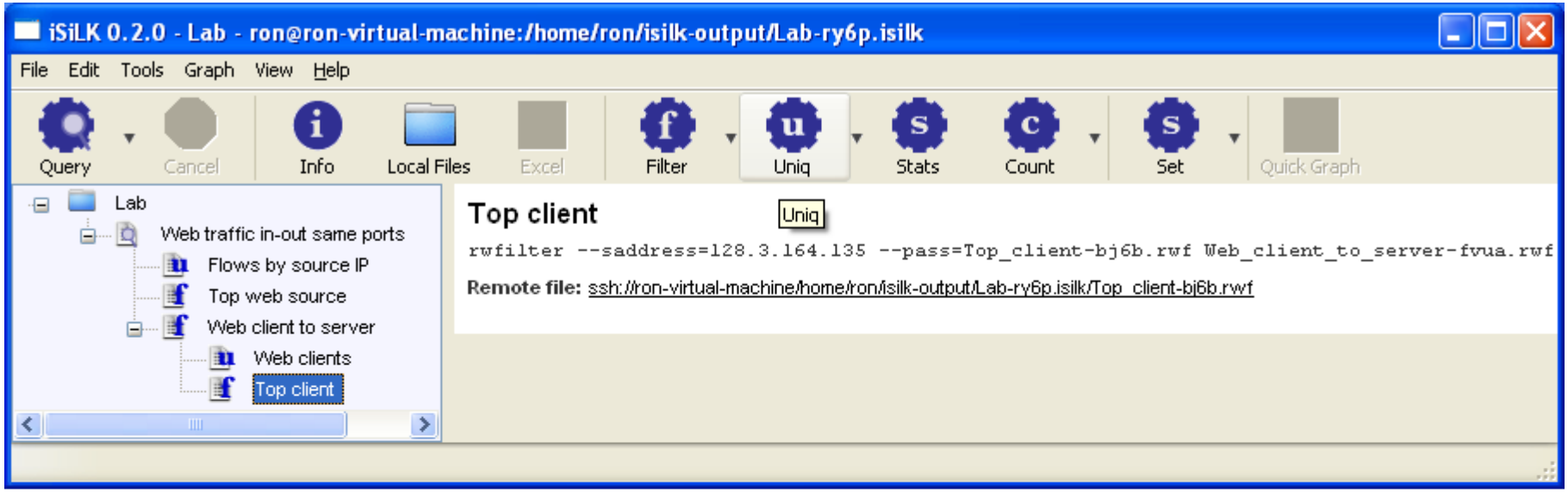

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Web clients
rwuniq Web_client_to_server-fvua.rwf --fields=sip --output-path=Web_clients-5g01.asc --flows
Local file: C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Web_clients-5g01.asc
sip records
0 92.3.250.2 5
1 59.79.251.254 4
2 131.243.92.247 141
3 56.96.15.108 2
4 208.78.202.125 9
5 128.3.211.229 4
6 56.96.15.127 39
7 128.3.45.232 254
8 131.243.93.18 7
9 160.131.231.235 3
10 131.243.203.159 4
11 131.243.94.180 36
12 131.243.155.24 33
13 131.243.219.196 1
14 151.68.53.231 1
15 59.79.251.253 5
16 59.79.251.1 8
17 131.243.92.99 1
18 128.3.112.153 2
19 148.92.15.67 7
20 136.176.162.189 3
1,890 records - C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Web_clients-5g01.asc

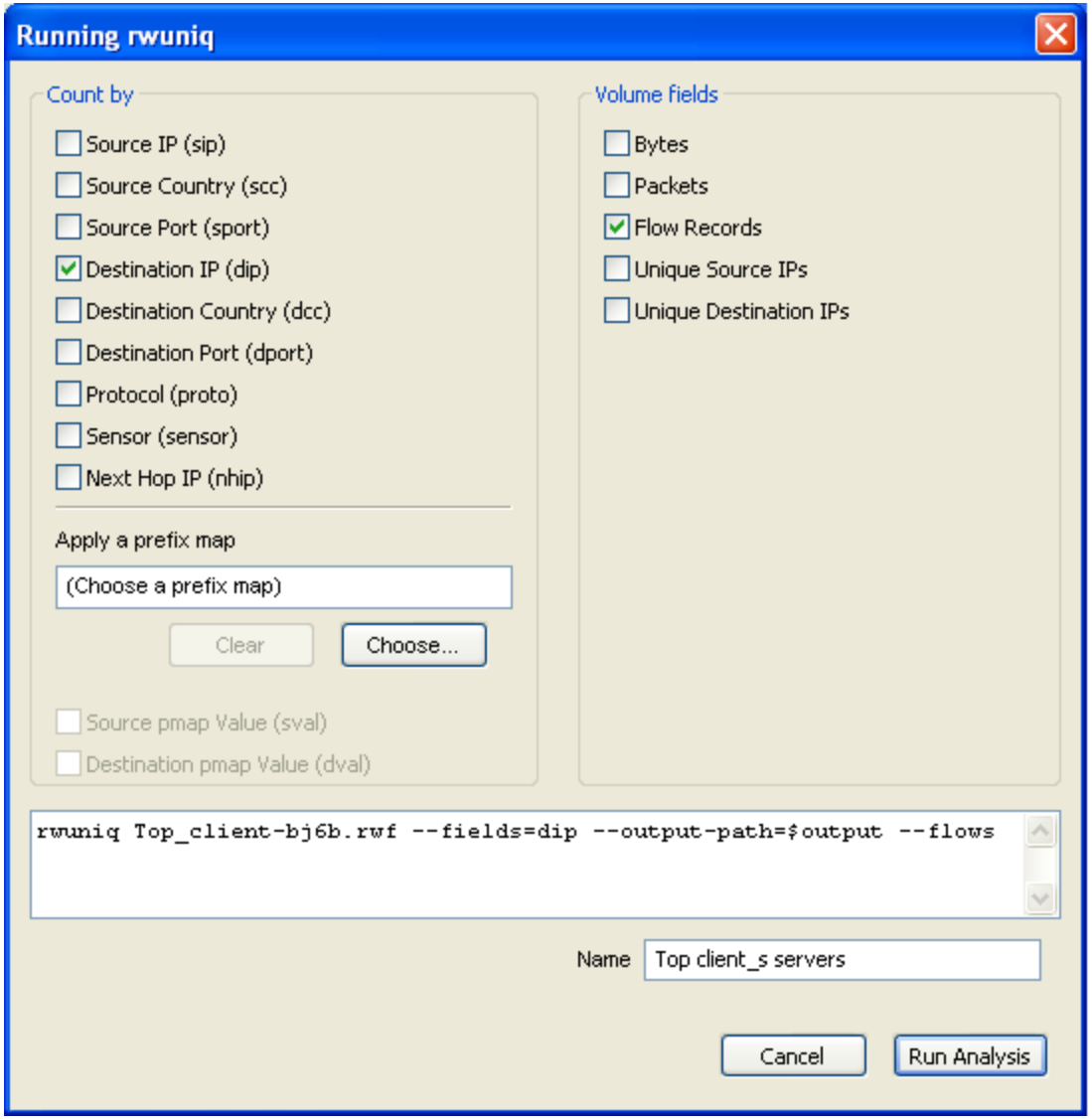

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Web clients
rwuniq Web_client_to_server-fvua.rwf --fields=sip --output-path=Web_clients-5g01.asc --flows
Local file: C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Web_clients-5g01.asc
sip records
125 128.3.164.135 6,605
388 128.3.48.71 5,041
1472 128.3.164.229 3,574
717 131.243.125.40 3,140
1758 128.3.96.153 3,105
900 131.243.93.121 1,757
700 148.240.109.182 1,673
544 128.3.255.49 1,429
1517 131.243.219.40 1,184
1555 131.243.141.86 1,077
891 131.243.141.208 952
1763 128.3.161.200 936
403 128.3.78.233 812
1834 131.243.125.92 772
128 128.3.255.17 700
550 131.243.219.202 697
148 128.3.48.38 650
24 131.243.142.239 646
322 131.243.93.87 617
243 131.243.12.210 611
1753 131.243.140.103 586


iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Filter
Web client to serv
rwfilter --dport=80,8080,443 --proto=6 --pass=Web_client_to_server-fvua.rwf
Web_traffic_in-out_same_ports-y6ha.rwf
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Web_client_to_server-fvua.rwf

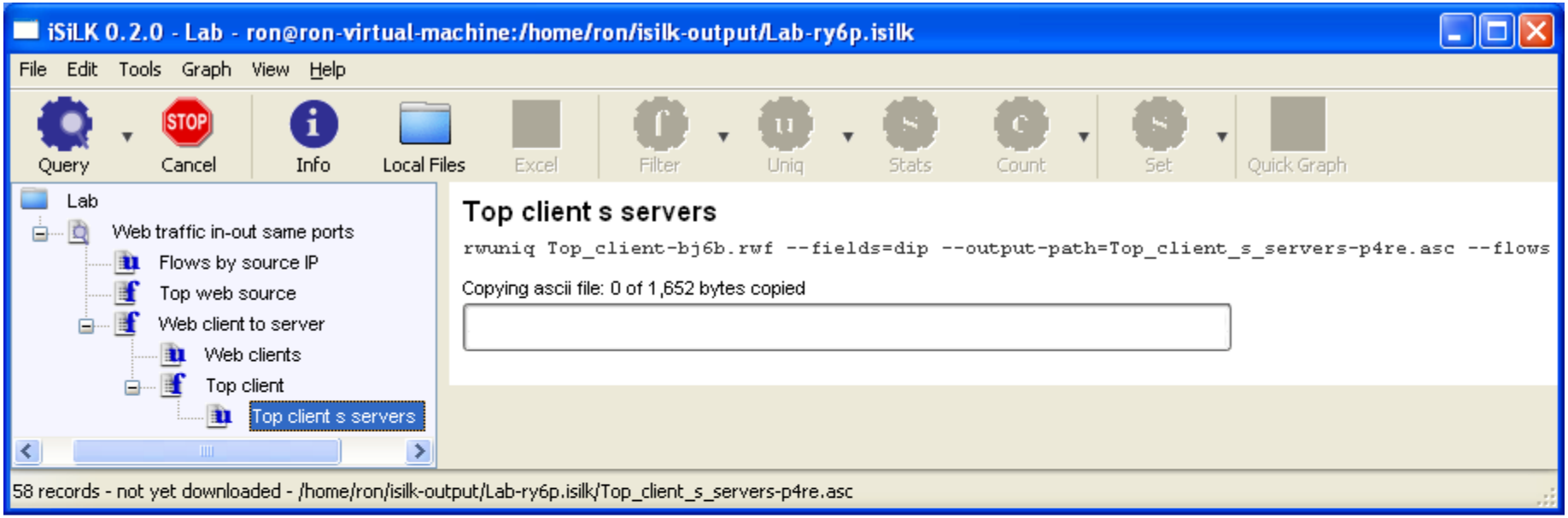

Running rwfilter drilldown
Basic Filter Options
Other Filter Options
IP Addresses and Ports
Filter based on source and destination
Source
IP
128.3.164.135
IP Set
(Choose a set)
Clear
Choose...
Port
0-65535
Destination
IP
x.x.x.x
IP Set
(Choose a set)
Clear
Choose...
Port
0-65535
Apply a Prefix Map
File
(Choose a prefix map)
Clear
Choose...
saddress
daddress
Country Codes
Source
Dest
Command line
rwfilter Web_client_to_server-fvua.rwf --saddress=128.3.164.135 --pass=$output
Name
Top client
Validate Options
Cancel
Run Analysis

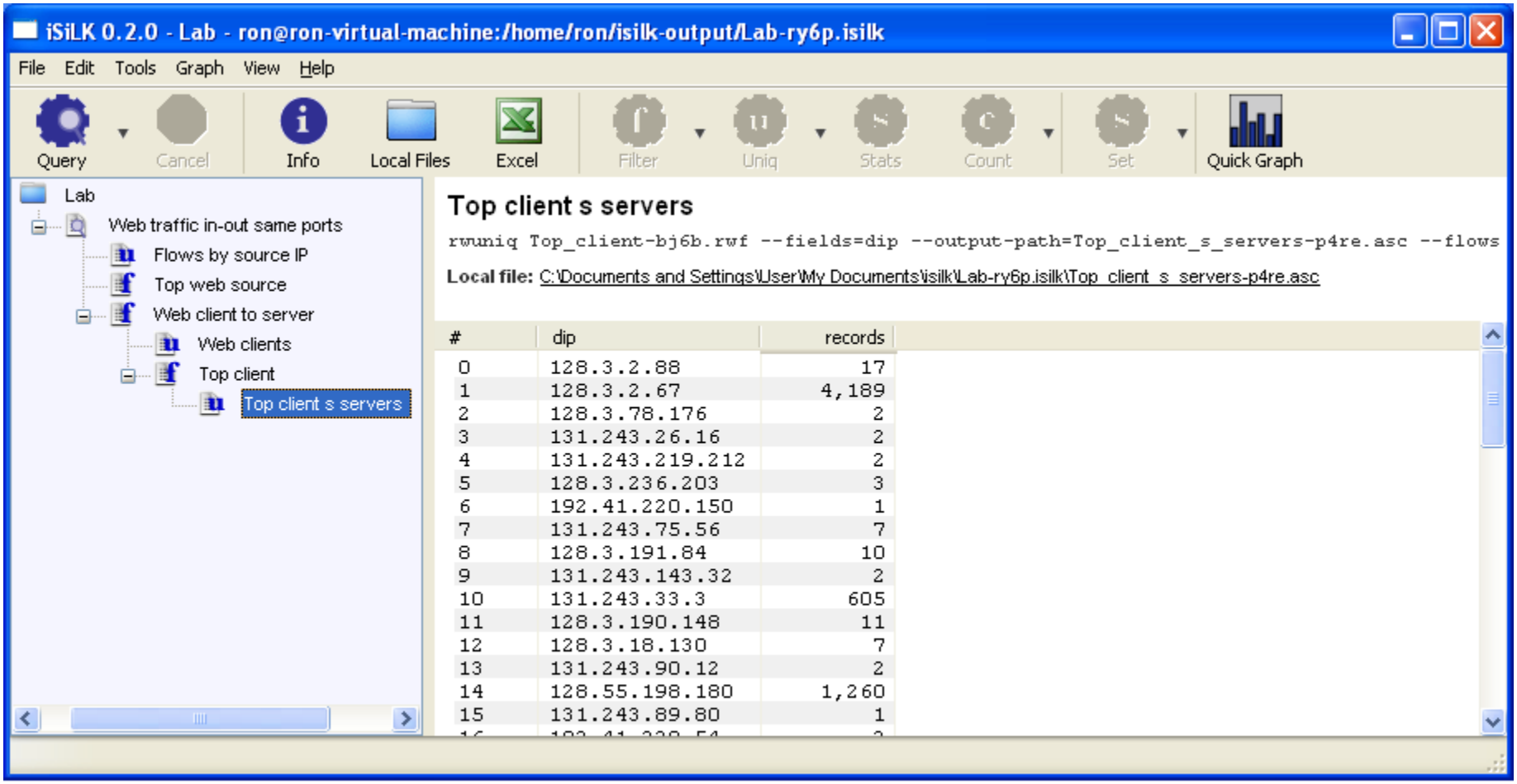

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client
rwfilter --saddress=128.3.164.135 --pass=Top_client-bj6b.rwf Web_client_to_server-fvua.rwf
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_client-bj6b.rwf
6,605 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Top_client-bj6b.rwf

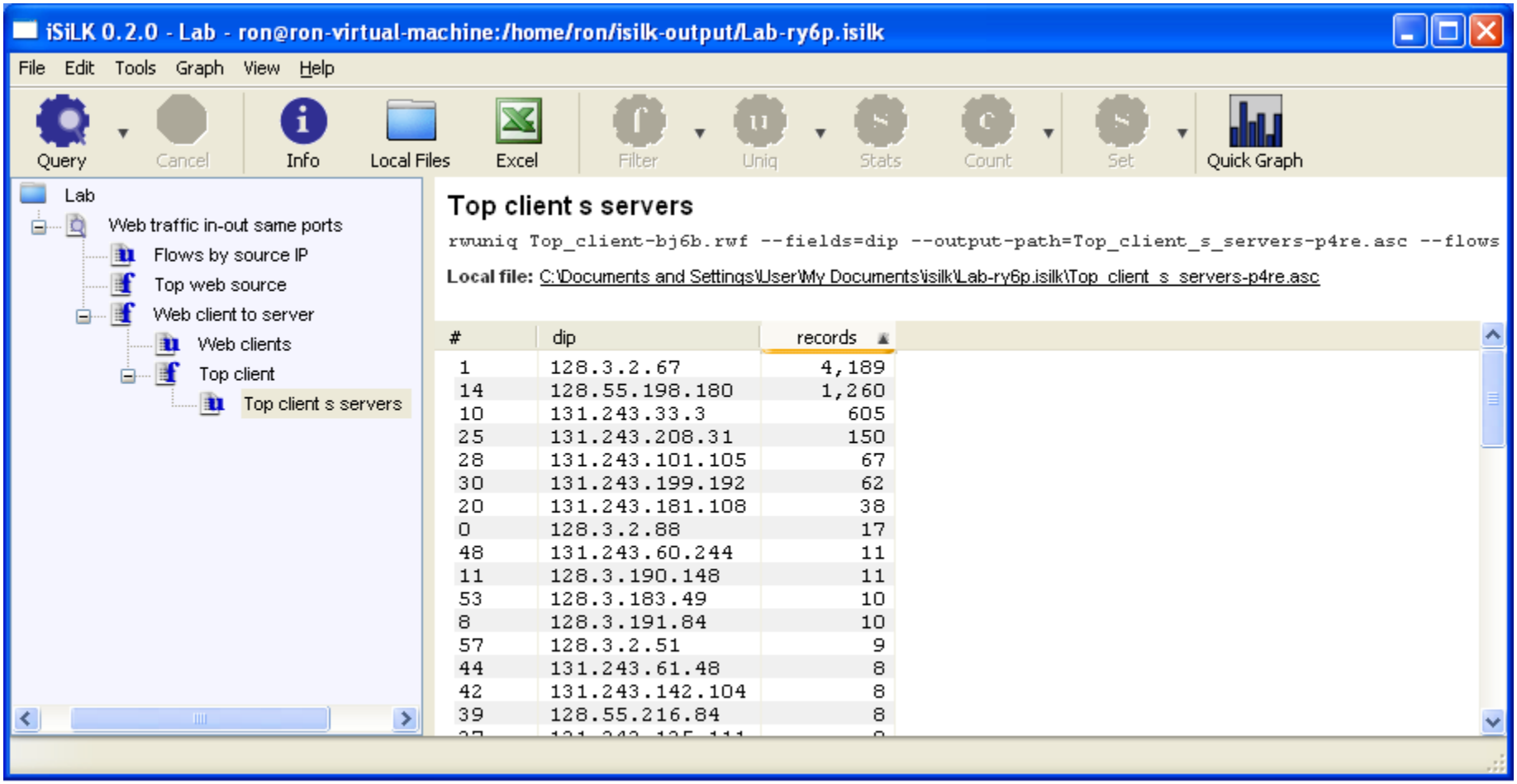

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client
Uniq
rwfilter --saddress=128.3.164.135 --pass=Top_client-bj6b.rwf Web_client_to_server-fvua.rwf
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_client-bj6b.rwf

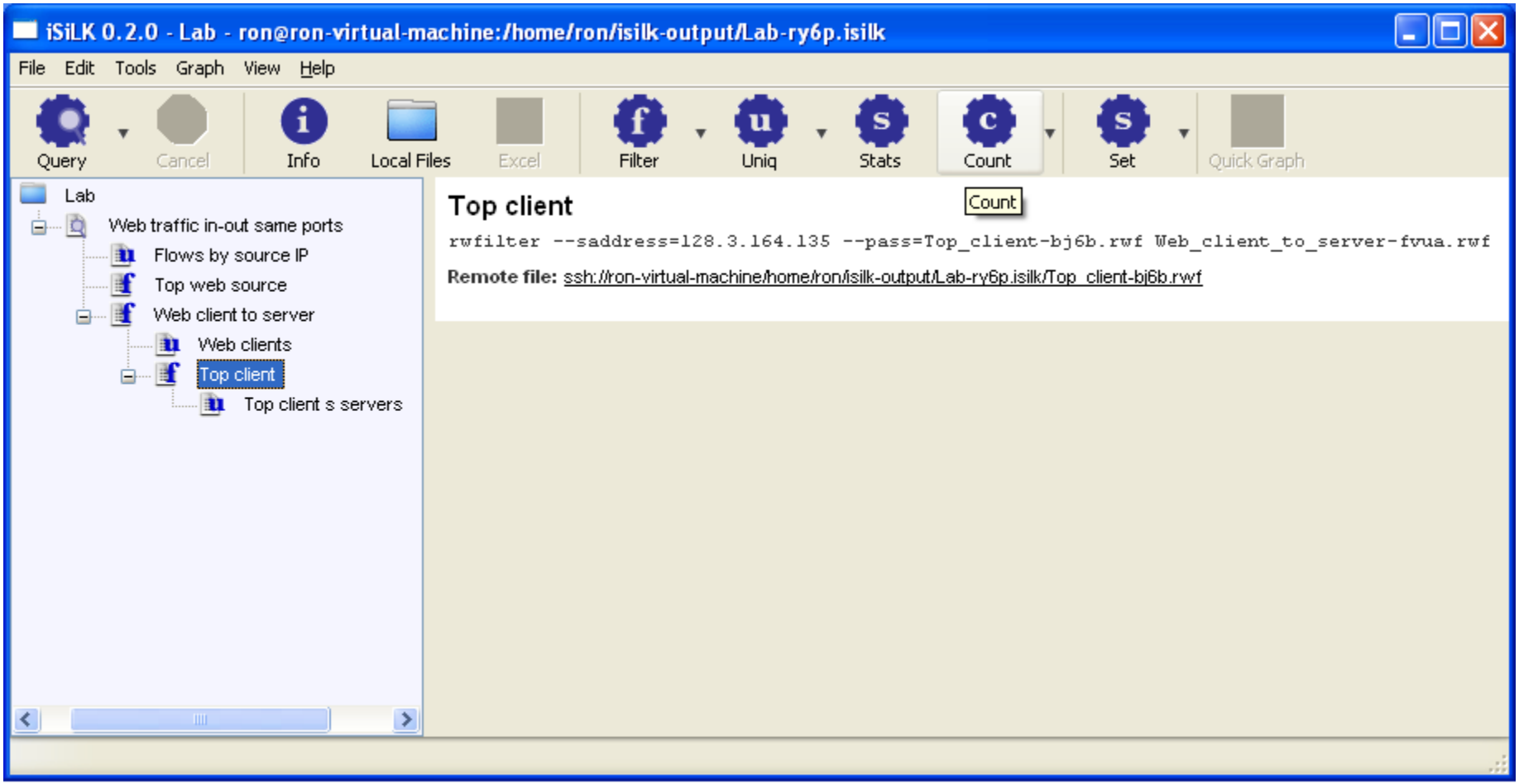

Running rwuniq
Count by
Source IP (sip)
Source Country (scc)
Source Port (sport)
Destination IP (dip)
Destination Country (dcc)
Destination Port (dport)
Protocol (proto)
Sensor (sensor)
Next Hop IP (nhip)
Apply a prefix map
(Choose a prefix map)
Clear
Choose...
Source pmap Value (sval)
Destination pmap Value (dval)
Volume fields
Bytes
Packets
Flow Records
Unique Source IPs
Unique Destination IPs
rwuniq Top_client-bj6b.rwf --fields=dip --output-path=$output --flows
Name
Top client_s servers
Cancel
Run Analysis

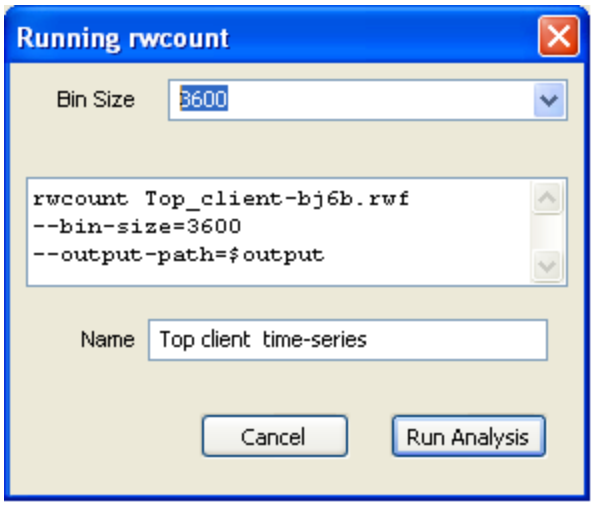

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client s servers
rwuniq Top_client-bj6b.rwf --fields=dip --output-path=Top_client_s_servers-p4re.asc --flows
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_client_s_servers-p4re.asc
58 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Top_client_s_servers-p4re.asc

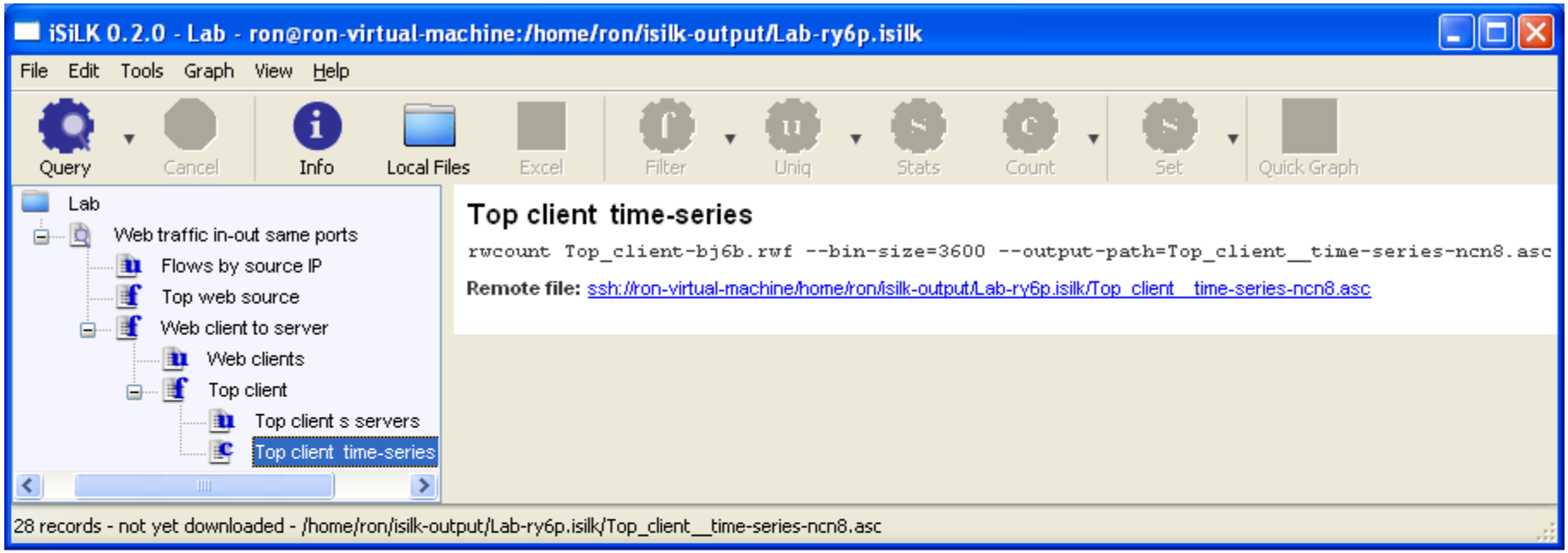

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client s servers
rwuniq Top_client-bj6b.rwf --fields=dip --output-path=Top_client_s_servers-p4re.asc --flows
Copying ascii file: 0 of 1,652 bytes copied
58 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Top_client_s_servers-p4re.asc

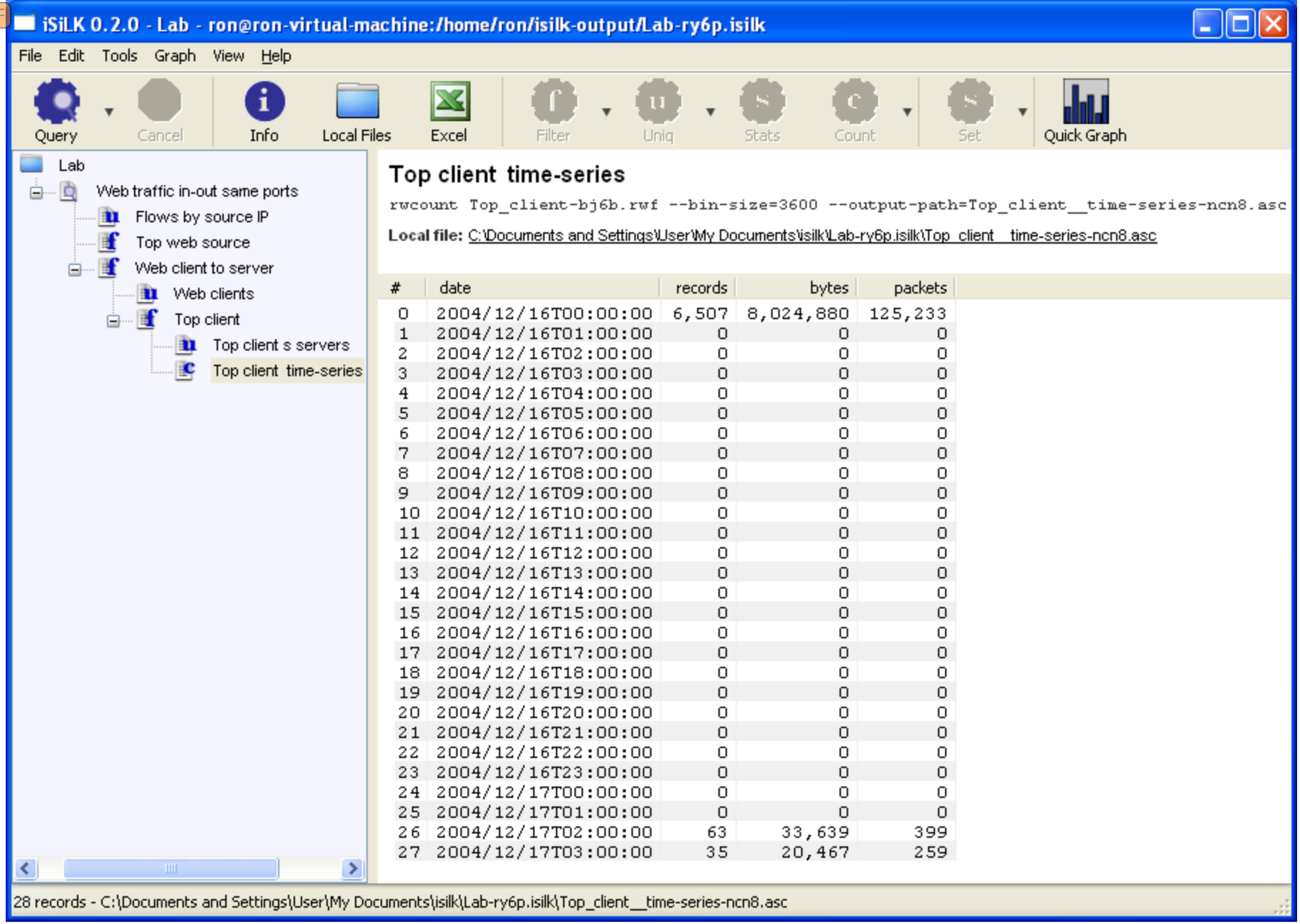

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client s servers
rwuniq Top_client-bj6b.rwf --fields=dip --output-path=Top_client_s_servers-p4re.asc --flows
Local file: C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Top_client_s_servers-p4re.asc
dip records
0 128.3.2.88 17
1 128.3.2.67 4,189
2 128.3.78.176 2
3 131.243.26.16 2
4 131.243.219.212 2
5 128.3.236.203 3
6 192.41.220.150 1
7 131.243.75.56 7
8 128.3.191.84 10
9 131.243.143.32 2
10 131.243.33.3 605
11 128.3.190.148 11
12 128.3.18.130 7
13 131.243.90.12 2
14 128.55.198.180 1,260
15 131.243.89.80 1


iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client s servers
rwuniq Top_client-bj6b.rwf --fields=dip --output-path=Top_client_s_servers-p4re.asc --flows
Local file: C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Top_client_s_servers-p4re.asc
dip records
1 128.3.2.67 4,189
14 128.55.198.180 1,260
10 131.243.33.3 605
25 131.243.208.31 150
28 131.243.101.105 67
30 131.243.199.192 62
20 131.243.181.108 38
0 128.3.2.88 17
48 131.243.60.244 11
11 128.3.190.148 11
53 128.3.183.49 10
8 128.3.191.84 10
57 128.3.2.51 9
44 131.243.61.48 8
42 131.243.142.104 8
39 128.55.216.84 8

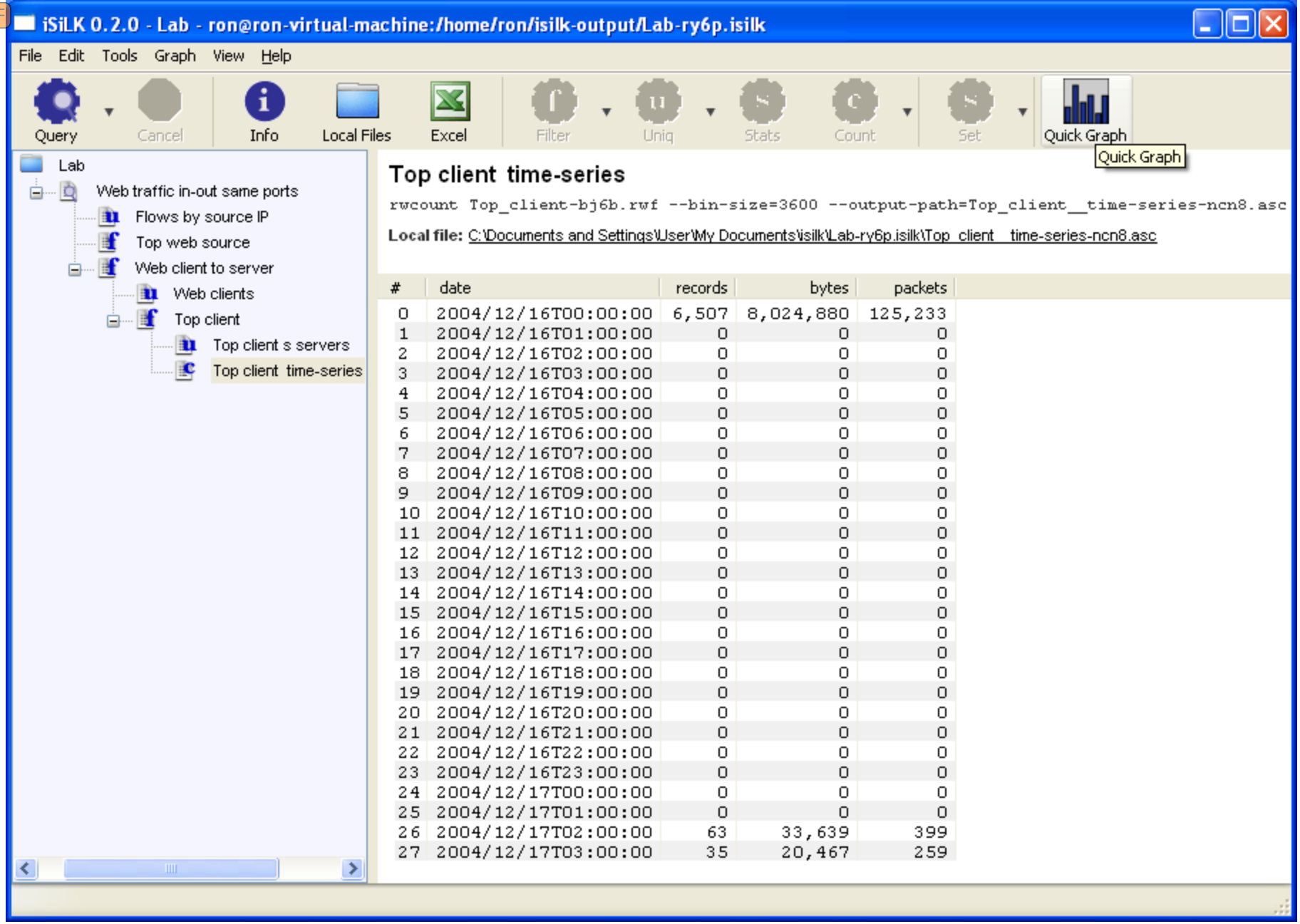

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client
Count
rwfilter --saddress=128.3.164.135 --pass=Top_client-bj6b.rwf Web_client_to_server-fvua.rwf
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_client-bj6b.rwf


Running rwcount
Bin Size
3600
rwcount Top_client-bj6b.rwf
--bin-size=3600
--output-path=$output
Name
Top client time-series
Cancel
Run Analysis

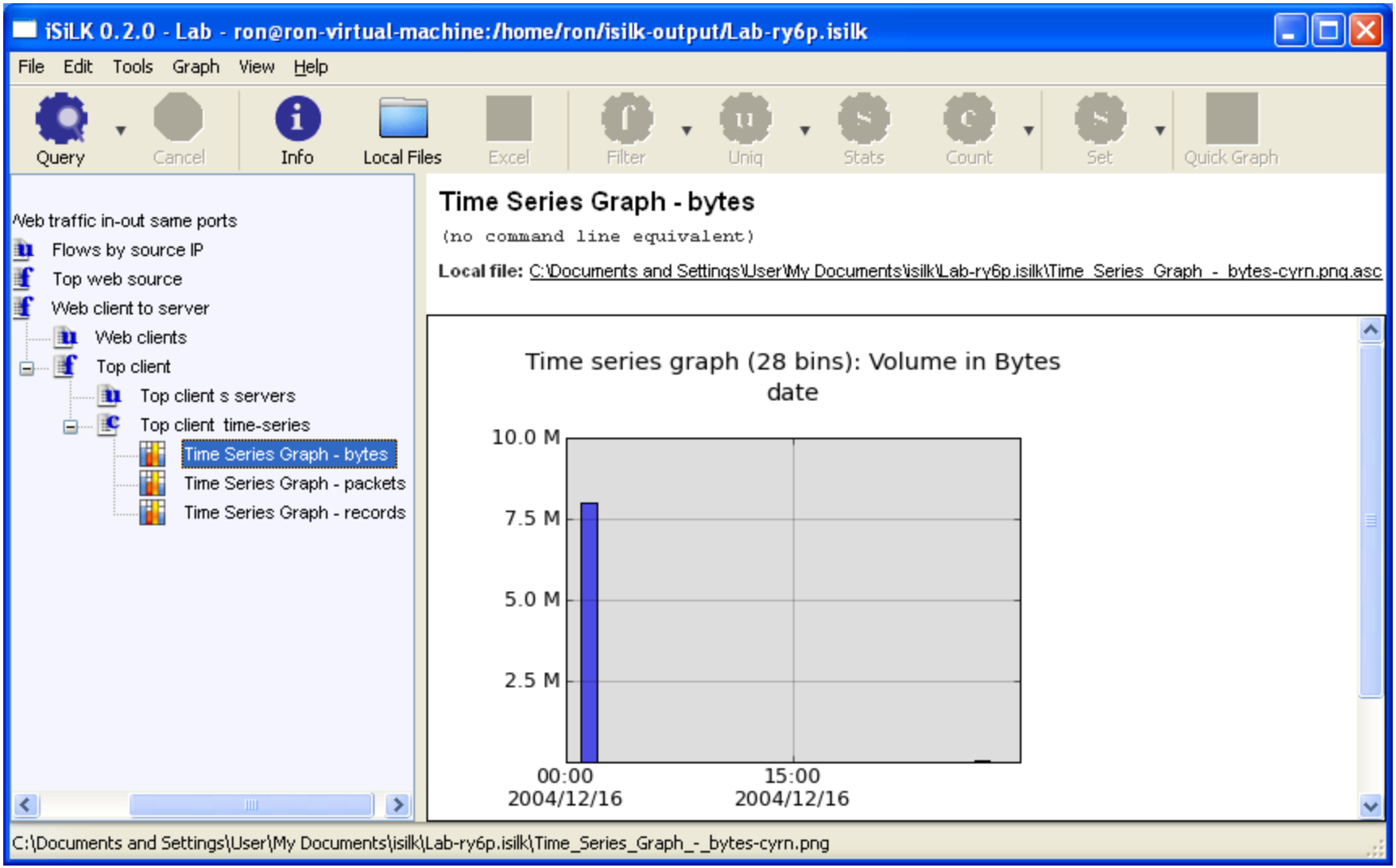

iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Lab
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client time-series
Top client time-series
rwcount Top_client-bj6b.rwf --bin-size=3600 --output-path=Top_client__time-series-ncn8.asc
Remote file: ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_client__time-series-ncn8.asc
28 records - not yet downloaded - /home/ron/isilk-output/Lab-ry6p.isilk/Top_client__time-series-ncn8.asc

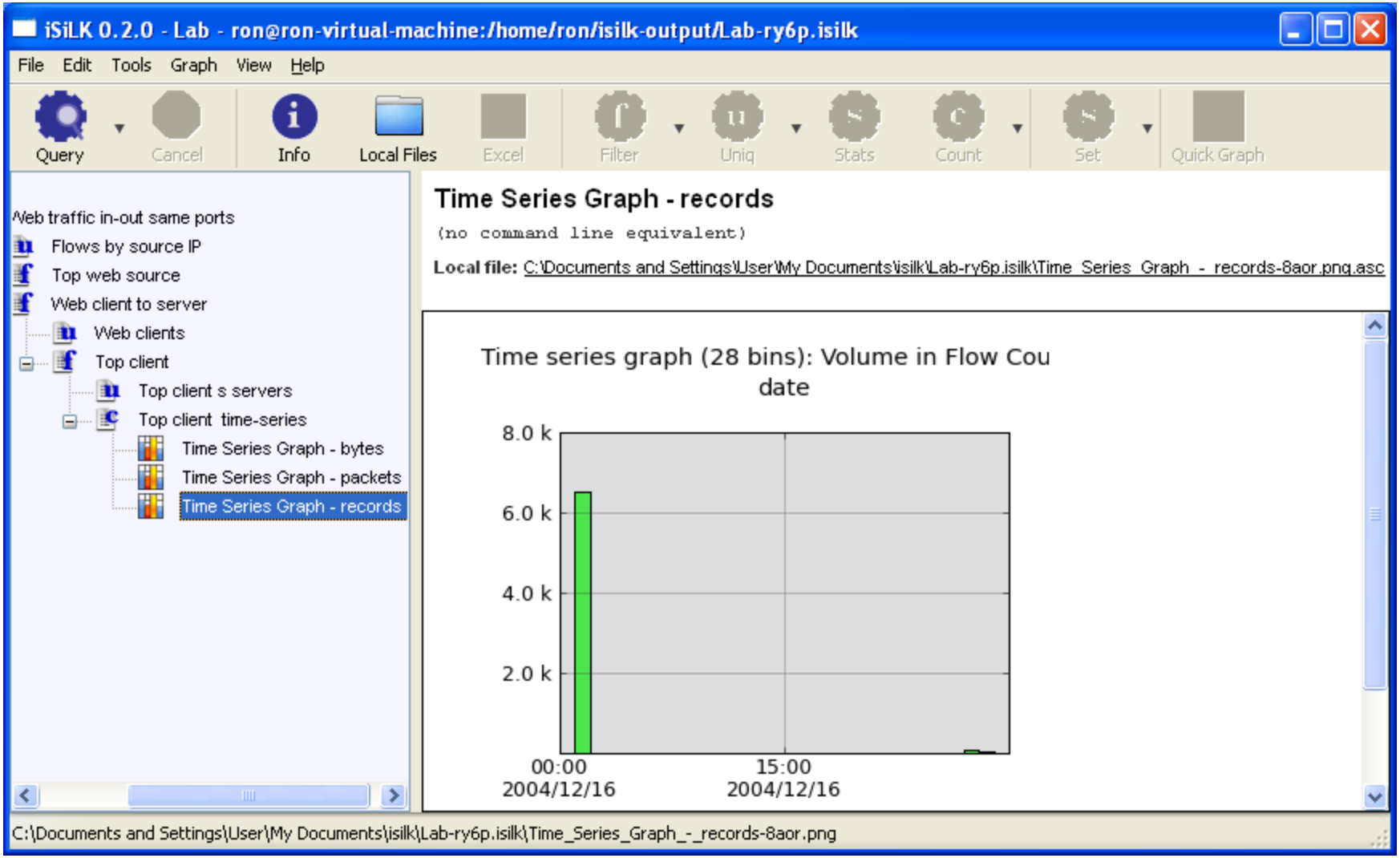


#	date	records	bytes	packets
0	2004/12/16T00:00:00	6,507	8,024,880	125,233
1	2004/12/16T01:00:00	0	0	0
2	2004/12/16T02:00:00	0	0	0
3	2004/12/16T03:00:00	0	0	0
4	2004/12/16T04:00:00	0	0	0
5	2004/12/16T05:00:00	0	0	0
6	2004/12/16T06:00:00	0	0	0
7	2004/12/16T07:00:00	0	0	0
8	2004/12/16T08:00:00	0	0	0
9	2004/12/16T09:00:00	0	0	0
10	2004/12/16T10:00:00	0	0	0
11	2004/12/16T11:00:00	0	0	0
12	2004/12/16T12:00:00	0	0	0
13	2004/12/16T13:00:00	0	0	0
14	2004/12/16T14:00:00	0	0	0
15	2004/12/16T15:00:00	0	0	0
16	2004/12/16T16:00:00	0	0	0
17	2004/12/16T17:00:00	0	0	0
18	2004/12/16T18:00:00	0	0	0
19	2004/12/16T19:00:00	0	0	0
20	2004/12/16T20:00:00	0	0	0
21	2004/12/16T21:00:00	0	0	0
22	2004/12/16T22:00:00	0	0	0
23	2004/12/16T23:00:00	0	0	0
24	2004/12/17T00:00:00	0	0	0
25	2004/12/17T01:00:00	0	0	0
26	2004/12/17T02:00:00	63	33,639	399
27	2004/12/17T03:00:00	35	20,467	259



#	date	records	bytes	packets
0	2004/12/16T00:00:00	6,507	8,024,880	125,233
1	2004/12/16T01:00:00	0	0	0
2	2004/12/16T02:00:00	0	0	0
3	2004/12/16T03:00:00	0	0	0
4	2004/12/16T04:00:00	0	0	0
5	2004/12/16T05:00:00	0	0	0
6	2004/12/16T06:00:00	0	0	0
7	2004/12/16T07:00:00	0	0	0
8	2004/12/16T08:00:00	0	0	0
9	2004/12/16T09:00:00	0	0	0
10	2004/12/16T10:00:00	0	0	0
11	2004/12/16T11:00:00	0	0	0
12	2004/12/16T12:00:00	0	0	0
13	2004/12/16T13:00:00	0	0	0
14	2004/12/16T14:00:00	0	0	0
15	2004/12/16T15:00:00	0	0	0
16	2004/12/16T16:00:00	0	0	0
17	2004/12/16T17:00:00	0	0	0
18	2004/12/16T18:00:00	0	0	0
19	2004/12/16T19:00:00	0	0	0
20	2004/12/16T20:00:00	0	0	0
21	2004/12/16T21:00:00	0	0	0
22	2004/12/16T22:00:00	0	0	0
23	2004/12/16T23:00:00	0	0	0
24	2004/12/17T00:00:00	0	0	0
25	2004/12/17T01:00:00	0	0	0
26	2004/12/17T02:00:00	63	33,639	399
27	2004/12/17T03:00:00	35	20,467	259


iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client time-series
Time Series Graph - bytes
Time Series Graph - packets
Time Series Graph - records
Time Series Graph - bytes
(no command line equivalent)
Local file: C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Time_Series_Graph_-_bytes-cyrn.png.asc
Time series graph (28 bins): Volume in Bytes
date
10.0 M
7.5 M
5.0 M
2.5 M
00:00
2004/12/16
15:00
2004/12/16
C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Time_Series_Graph_-_bytes-cyrn.png


iSiLK 0.2.0 - Lab - ron@ron-virtual-machine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View Help
Query
Cancel
Info
Local Files
Excel
Filter
Uniq
Stats
Count
Set
Quick Graph
Web traffic in-out same ports
Flows by source IP
Top web source
Web client to server
Web clients
Top client
Top client s servers
Top client time-series
Time Series Graph - bytes
Time Series Graph - packets
Time Series Graph - records
Time Series Graph - records
(no command line equivalent)
Local file: C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Time_Series_Graph_-_records-8aor.png.asc
Time series graph (28 bins): Volume in Flow Cou
date
8.0 k
6.0 k
4.0 k
2.0 k
00:00
2004/12/16
15:00
2004/12/16
C:\Documents and Settings\User\My Documents\isilk\Lab-ry6p.isilk\Time_Series_Graph_-_records-8aor.png

Labs

Questions?

Contact Information

Ron Bandes, **rbandes@cert.org**

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA