

Network Analysis with iSiLK

Presented at FloCon[®] 2011

Ron Bandes CERT[®] Network Situational Awareness (NetSA) Group NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at <u>permission@sei.cmu.edu</u>.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

CERT[®] is a registered mark owned by Carnegie Mellon University.



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





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











Packet Encapsulation













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

























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





iSiLK environment



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 \rightarrow Programming \rightarrow iSiLK iSiLK Configuration: Remote_Host: localhost (default) 22 (default) Remote_Port: Remote_User: liveuser RSH_Key: /home/liveuser/.ssh/id_rsa Rmt_Output: isilk-output isilk-libs Rmt_Library:

First Screen — Problem Sets

 $\overline{\mathbf{F}}$

iS	SiLK - Problem Sets		
ſ	My Problem Sets Remote Problem Sets		
	Found the following problem sets:		
	Problem Set	Directory	Date Modified
	fool	C:\Documents and Settings\User\My Documents\isilk\fool-s4pa.isilk	Nov 09 2010, 02:42 PM
	<	III	>
	<u>N</u> ew		Open Quit





iSiLl	(0.2.() - fool -	ron@ro	n-virtual-m	achine:isilk-output	t/fool-s4pa	.isilk			
File Edi	t Tool:	; Graph	View <u>H</u> e	elp						
Query	•	Cancel	i Info	D Local Fi	les Excel	Filter	Uniq .	Stats	Count	Set
	fool				iSiLK - fool Local directory: Remote directory:	<u>C:\Document</u> ssh://ron-virt	s and Settings ual-machineis	s\User\My Do ilk-output/foc	ocuments'iisilk'i ol-s4pa.iisilk	fool-s4pa.isilk
C:\Docum	ents an	d Settings'	(User\My D	ocuments\isilk	\fool-s4pa.isilk					





🔲 Query Builder (fool-s4pa.is	ilk)	
Basic Query Options More Filter Opt	ions	
Data files to search	IP Addresses and Ports	
Data Pool (class/type)	Incoming V Filter based on source an	nd destination
	Source	
Sensors	All Sensors V Choose IP X.X.X.X	
Time Range to Query	IP Set (Choose a	set)
Nov v 2010 v		Clear Choose
	Port 0.65535	
S M T W T F S	S M T W T F S Point 0-00000	· · · · · · · · · · · · · · · · · · ·
	7 8 9 10 11 12 13	
14 15 16 17 18 19 20	14 15 16 17 18 19 20	
21 22 23 24 25 26 27	21 22 23 24 25 26 27 IP Set (Choose a)	set)
28 29 30	28 29 30	
		Clear Choose
Start hour (GMT): 21 🛟	End hour (GMT): 21	
Selected 1 hour	Port 0-65535	~
rwfiltertype=in,inweb ·	start-date=2010/11/10:21proto=0-255pass=	\$output
Name Untitle	ed Query Add to fool-s4pa.isilk	Return records that FAIL filter
Valida	ate Options Save As Plugin Cl	ose Run Remote Query



Query Builder—more filter options

	5	
Apply a Prefi	< Map	Protocol and protocol-specific fields
File	(Choose a prefix map)	Protocol 0-255
	Clear Choose	FSRPAUEC TCPFlags
saddress		ICMP Type 0-255
daddress		ICMP Code 0-255
Dest		b/p 1-
filtert	ype=in,inwebstart-date=2010/11/J	LO:21proto=0-255pass=\$output
	Name Untitled Query	Add to fool-s4pa.isilk







Query Builder (LBNL-62eu.isilk)

Basic Query Options More Filter Opt	ions	
Data files to search		CIP Addresses and Ports
Data Pool (class/type)		Filter based on source and destination
Sensors		Source
5015015	All Sensors Y Choose	IP x.x.x.x
Time Dense he Overw		IP Set (Choose a set)
Time Range to Query	Custom	
Dec 💙 2004 💙	Dec 💙 2004 💙	Clear Choose
		Port 80,8080,443
		Destination
5 6 7 8 9 10 11 12 13 14 15 16 17 18	5 6 7 8 9 10 11	IP X.X.X
	19 20 21 22 23 24 25	
		IP Set (Choose a set)
		Clear Choose
Start bour (GMT): 0	End hour (GMT): 23	
		Port 80,8080,443
2 days U hours		
rwfiltertype=out,outweb dport=80,8080,443spon),in,inwebstart-date=200 rt=80,8080,443pass=\$outp	4/12/16:00end-date=2004/12/17:23
Norro Wah k	raffic in out came parts	
Name web t	rame in-out same ports Add to	LDIVL-62eu.ISIIK
Valida	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 2004/12/16:12 2004/12/16:13 2004/12/16:15 2004/12/16:15 2004/12/17:04 2004/12/17:05 2004/12/17:06 2004/12/17:08 2004/12/17:09 2004/12/17:10
Yes No









ata files	to sea	arch -											1	IP Ad	Idresses	and Ports	
)ata Pool	(class	;/typ	e)			All						*		J	lter base	ed on source and destination	
			Se	enso	rs	All Se	ensoi	rs 🔹	~ [Ch	oose		2	Sourc	e or Des	tination	
								-		- Crit	0000				IP	X.X.X.X	
lime Ranı	ge to (Ouer	v			0.00	0.000								IP Set	(Choose a set)	
Dec	1	2	2004	*]	Dec	.om	•	~	2004	- ~					Clear Choose	·
SM	T	W	ΤI	F	s	s	M	Т	W	Т	F	S			Port	80,8080,443	
		1	2	3	4	É			1	2	3	4	0	Destir	nation		
12 13	7	8	9	10	11 1º	12	6 1 2	7	8	9	10	11			IP	x.x.x.x	
19 20) 21	22	23	24	25	19	20	21	22	23	24	25				(Choose a set)	
26 27	28	29	30	31		26	27	28	29	30	31				ir oct		
																Clear Choose	
Start hou 2 days 0	ur (GM hours	IT): [0	v		End l	nour	(GM1	r): [23	v				Port	80,8080,443	
filter	t3	npe=	out	,ou	twel	b,in,	inw	eb ·	st	tart	t-ds	ate=2	004/	12/1	L6:00	end-date=2004/12/17:23	
aport=8	30,80	080,	443		pas	s=\$ou	tpu	t									
													_				
			Nam	e V	Veb t	traffic i	n-ou	t sam	ne po	orts		Add	to LE	BNL-6	2eu.isilk	💌 📔 Return records that F	AIL Í











Running rwuniq	X
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 output-path=\$outputflows	-eugb.rwffields=sip
	Name Flows by Source IP Cancel Run Analysis









INDEK U. 2.0 - LUNL - ron@ron-virtual ile Edit Tools Graph View <u>H</u> elp	-machine	:/home/ron/isilk-output/L	BNL-6Zeu.isilk		
Query Cancel Info Local	Files Ex	Kcel Filter	g • Stats	Count Set	▼ Juick Graph
 LBNL Web traffic in-out same ports Flows by Source IP 	Flow rwunid outy Local fi	s by Source IP q Web_traffic_in-out_sa put-path=Flows_by_Source Ne: <u>C:VDocuments and SettingsV</u>	ame_ports-eugh :e_IP-og0z.asc JserWMy Documents	o.rwffields=sip 2flows SVisilk/LBNL-62eu.isilk/Flows b	y Source IP-oq0z.e
	#	sin	records		
		02 2 250 2	E		
	1	50 70 251 254	<u>م</u>		
	2	118 133 0 234	4		
	3	220 80 248 135	1		
	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		
	q	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		

File Edit T	<mark>2.0 - LBNL - ron@ron-virt</mark> ools Graph View <u>H</u> elp	ual-machine:	/home/ron/isilk-output/L	BNL-62eu.isilk	
Query .	Cancel Info Lo	cal Files Exi	G Filter	iq • Stats	Count Set Quick Graph
181 ==	VL Web traffic in-out same ports Web traffic in-out same ports Web traffic in-out same ports 	Flows rwuniq outp Local file	by Source IP Web_traffic_in-out_s: ut-path=Flows_by_Source e: <u>C:VDocuments and SettingsV</u>	ame_ports-eugb ce_IP-og0z.asc JserWy Documents	.rwffields=sip :flows Yisik¥LBNL-62eu.isik¥Flows by Source IP-oqOz.
		#	sip	records 🔳	
		423	131.243.15.56	6,970	
		437	128.3.164.135	6,605	
		2.53	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	
		2066	121 242 141 209	952	
1		<u> </u>	131.243.141.200	204	

(_		
	-		
4		_	
	\mathbf{V}		

Running rwfilter drilldown
Basic Filter Options Other Filter Options
Protocol and protocol-specific fields
Protocol 3
All (0-255)
Common (1,6,17)
UDP (17)
ICMP T TCP (6)
SCTP (132)
IGMP (2)
IGP (9)
Flow size fields
Buteo 1.
Dyles I ⁻
Pkts 1-
b/p 1-
Command line
rwfilter Web_traffic_in-out_same_ports-eugb.rwfsaddress=131.243.15.56dport=80,8080,443
proco-6pass-voucpuc
Name Uptitled Definement
Validate Options Cancel Run Analysis





Running rwfilter drilldown	×
Basic Filter Options Other Filter Options	
IP Addresses and Ports	Apply a Prefix Map
	File (Choose a prefix map)
IP 131.243.15.56	Clear Choose
IP Set (Choose a set)	
Clear Cho	ose
Port 0-65535	daddress
Destination	
IP X.X.X	Country Codes
IP Set (Choose a set)	Source V
Clear	ose Dest
Port 80,8080,443	
Command line	
proto=6pass=\$output	agb.rwfsaddress=131.243.15.56dport=80,8080,443
	Name Top web source
	Validate Options Cancel Run Analysis











Running rwfilter	drilldown	
Basic Filter Option	05 Other Filter Onlight	
The Addresses	Other Filter Options	Analyse Durffy Mar
Filter base	and Ports ed on source and destination	
Source		File (Choose a prefix map)
IP	x.x.x.x	Clear Choose
IP Set	(Choose a set)	
	Clear Choose	saddress
Port	0-65535	daddress
Destination		
IP	x.x.x.x	Country Codes
IP Set	(Choose a set)	Source
	Clear Choose	Dest 🗸
Port	80,8080,443	
Command line		
rwfilter Web_t	raffic_in-out_same_ports-y6ha.rwf	dport=80,8080,443proto=6pass=\$output
		Name Web client to server
		Validate Options Cancel Run Analysis











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 Hep ID (chip)	Volume fields Bytes Packets Flow Records Unique Source IPs Unique Destination IPs
Apply a prefix map (Choose a prefix map) Clear Choose Source pmap Value (sval) Destination pmap Value (dval)	
rwuniq Web_client_to_server-fvua.rwf output-path=\$outputflows	fields=sip
	Name Web clients Cancel Run Analysis





🔲 iSiLK	(<mark>0.2.0</mark> - La	ıb - ron@ror	ı-virtual-m	achine:/home	/ron/isilk-ou	utput/Lab-ry	6p.isilk				· 🗆 🔼
File Edit	t Tools Gra	aph View <u>H</u> e	lp:								
Query	Cance	el Info	Local Fi	les Excel	Filter	• Uniq	• Stats	Count	Set	Quick Graph	
	Lab Web t	traffic in-out sa Flows by source Top web source Web client to se the Web client	me ports ce IP ce erver ts	Web clier rwuniq Web flows Remote file:	nts _client_to <u>ssh://ron-virtua</u>	_server-fvu I-machine/home	a.rwffie Mron/isilk-output	≥lds=sip, Mab-ry6p.isikN	output-pat] Neb clients-5g	h=Web_clients-! <u>01.asc</u>	5g01.asc
<											
1,890 reco	ords - not yet	downloaded - /	/home/ron/isilk	-output/Lab-ry6p	o.isilk/Web_clier	nts-5g01.asc					





🔲 iSiLl	(0.2.0 - La	b - ron@ron	-virtual-m	achine:/home	/ron/isilk-o	utput/Lab-ry	6p.isilk				
File Edi	t Tools Gra	ph View <u>H</u> el	P								
Query	Cance	i Info	Local Fi	les Excel	O Filter	• Uniq	• Stats	Count	- Set	▼ Quick Graph	
	Lab VVeb tr 	raffic in-out san Tows by sourc Top web source Veb client to se Web client	ne ports e IP e rver s	Web clier rwuniq Web flows Remote file:	its _client_to ssh://ron-virtua	_server-fvu I-machine/home	a.rwffie e/ron/isilk-output	elds=sip t∕Lab-ry6p.isilk/	-output-pat	h=Web_clients 1 <mark>01.asc</mark>	-5g01.asc
1,890 rec	ords - not yet	downloaded - /ł	nome/ron/isilk	-output/Lab-ry6p).isilk/Web_clier	nts-5g01.asc					.;;



le Edit Tools Graph View <u>H</u> elp	achine:/h	omerron/istik-output/La	о-губр.тятк		
Query Cancel Info Local F	iles Exc	E D . C	iq • Stats	Count Set Quick Graph	
 Lab Web traffic in-out same ports Flows by source IP Top web source Web client to server 	Web c rwuniq flows Local file	c lients Web_client_to_server- s e: <u>C:VDocuments and SettingsV</u>	-fvua.rwff: JserWyDocuments	ields=sipoutput-path=Web_clients-5g01 <u>s\isilk\Lab-ry6p.isilk\Web clients-5g01.asc</u>	as
🏨 Web clients	#	sip	records		
	0	92 3 250 2	5		- 1
	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		
	10	149 02 15 67	7		
	19	140.94.13.07			
	19 20	136.176.162.189	3		



File Edit Tools Graph View <u>H</u> elp	al-machine:/ho	ome/ron/isilk-output/La	ıb-ry6p.isilk	
Query Cancel Info Lo	cal Files Exce	Filter Ur	iq Stats	Count Set Quick Graph
 Lab Web traffic in-out same ports Flows by source IP Top web source Web client to server 	Web c rwuniq flows Local file	lients Web_client_to_server : <u>C:Documents and SettingsV</u>	-fvua.rwff UserWhy Document	ields=sipoutput-path=Web_clients-5g0l.asc tsWsWkWab-rγ6p.isWkWVeb clients-5q01.asc
	#	sip	records 🔳	A
	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	
	4 T J			
	1753	131.243.140.103	586	







is trikes on th		
sic Filter Option	Other Filter Options	
-IP Addresses Filter base Source	and Ports ed on source and destination	Apply a Prefix Map File (Choose a prefix map)
IP	128.3.164.135	Clear Choose
IP Set	(Choose a set)	saddress
Port	0-65535	daddress
Destination		
IP	x.x.x.x	Country Codes
IP Set	(Choose a set)	Source
Port	0-65535	Dest
and line lter Web c	lient to server-fvua.rwfsaddres:	s=128.3.164.135pass=\$output
_		
		Name Top client
		Validata Optione Cancel Dup And





iSiLK 0.2.0 - Lab - ron@ron-virtual-n	nachine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View <u>H</u> elp	
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 	Top client rwfiltersaddress=128.3.164.135pass=Top_client-bj6b.rwf Web_client_to_server-fvua.rwf Remote file: <u>ssh://ron-virtual-machine/home/ron/isilk-output/Lab-ry6p.isilk/Top_client-bj6b.rwf</u>
Web clients Top client	ilk-outout/Lab-ry6p isilk/Top_cliept-bi6b rwf
of the second state of the	





iSiLK 0.2.0 - Lab - ron@ron-virtual-m 🖬	lachine:/home/ron/isilk-output/Lab-ry6p.isilk
File Edit Tools Graph View <u>H</u> elp	
Query Cancel Info Local F	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 	Top client Uniq rwfiltersaddress=128.3.164.135pass=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
Web clients	





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.rwffields=0	dipoutput-path=\$outputflows 🔥
	Name Top client_s servers Cancel Run Analysis

















iSiLK 0.2.0 - Lab - ron@ron-virtual-m	achine:/hom	e/ron/isilk-output/La	b-ry6p.isilk			
File Edit Tools Graph View <u>H</u> elp						
Query Cancel Info Local F	Files Excel	G . G	iq C	Count - S	Quick Graph	
🚞 Lab	Top clier	at e earvare				
🖕 🗋 Web traffic in-out same ports	Top clief	11 5 501 4015				
Elows by source IP	rwuniq Top	p_client-bj6b.rwf	fields=dip	output-path=Top_cl	lient_s_servers-p4re	.ascflows
	Local file: C:	Documents and Settings	UserWy Documer	nts\isilk\Lab-ry6p.isilk\Top_clie	nt s servers-p4re.asc	
				•••••	· · · · · ·	
Vveb client to server		dia	rocorde			
Web clients	#		records			
🚊 🥂 🛛 Top client	0 :	128.3.2.88	17			
Top client s servers	1 .	128.3.2.67	4,189			E .
	2	128.3.78.176	2			
	3.	131.243.25.15	4			
		131.243.219.212	4			
	5.	128.3.236.203	3			
	ь. 	192.41.220.150	1			
	· · ·	131.243.75.56	10			
	8.	128.3.191.84	10			
	9.	131.243.143.32	605			
	10 .	131.243.33.3	605			
	12 .	120.3.190.140	11			
	12 .	120.3.10.130	2			
	10 .	131.243.90.12	1 260			
	15	120.33.190.180	1,200			
	10 .	101.440.09.00	1			×
						.::





File Edit Tools Graph View Help Image: Problem 1 Image: Problem 2 <	J raph
Query Cancel Info Image: Local Files Image: Excel Image: Filter Image	raph
Lab Web traffic in-out same ports Top client s servers rwuniq Top_client-bj6b.rwffields=dipoutput-path=Top_client_s_servers-p4re.asc -	
Top web source IP	ers-p4re.ascflows <u>re.asc</u>
Web client to server	^
Image: Top client 1 128.3.2.67 4,189 Image: Top client s servers 14 128.55.198.180 1,260 Image: Top client s servers 10 131.243.33.3 605 25 131.243.208.31 150 28 131.243.101.105 67 30 131.243.181.108 38 0 128.3.2.88 17 11 128.3.190.148 11 13 128.3.190.148 11 13 128.3.191.84 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	
	×.







































Questions?





Contact Information

Ron Bandes, rbandes@cert.org

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA

