AND THEY SAID TO THE TITANS: « WATCH OUT OLYMPIANS IN THE HOUSE! »

CSEC – Advanced Network Tradecraft

SD Conference June 2012

Overall Classification: TOP SECRET//SI

OLYMPIA & THE CASE STUDY



OLYMPIA

CSEC's Network Knowledge Engine

Various data sources
Chained enrichments
Automated analysis

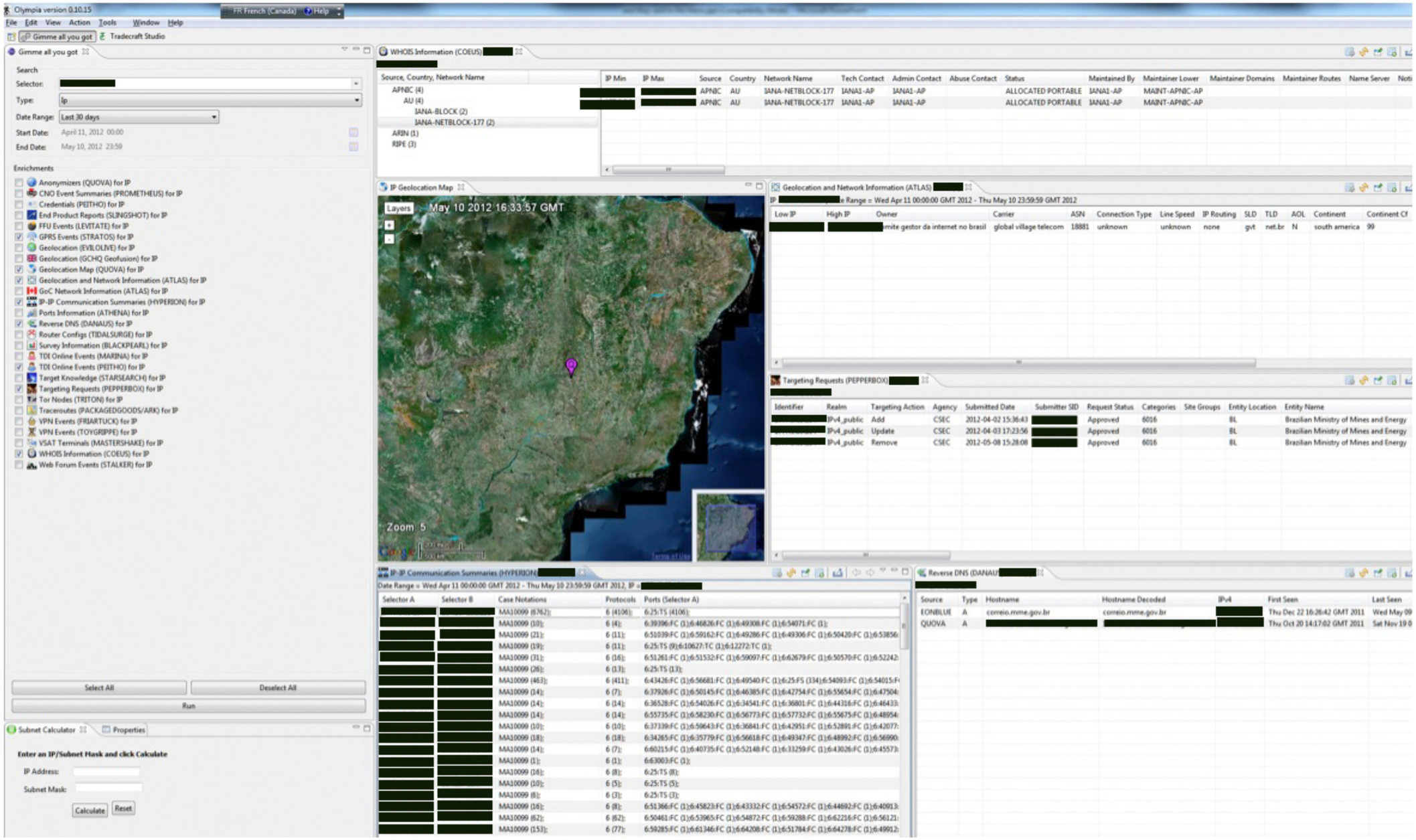
Brazilian Ministry of Mines and Energy (MME)

New target to develop
Limited access/target knowledge

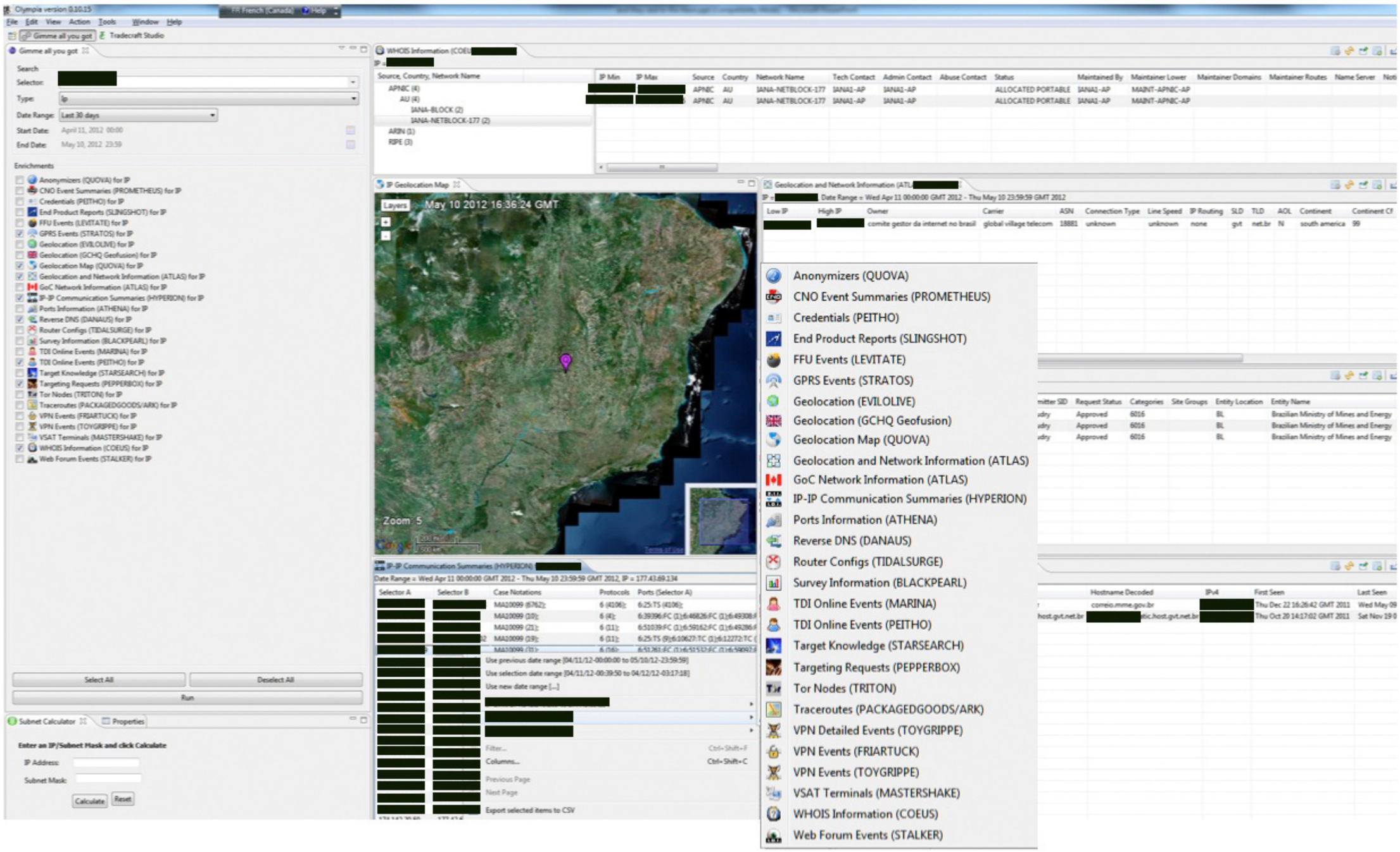
QUESTIONS

- How can I use the information available in SIGINT data sources to learn about the target?
- What can I find that would help me inform access development efforts?
- Can I automate the analytical process and/or re-use analytics designed for other purposes?

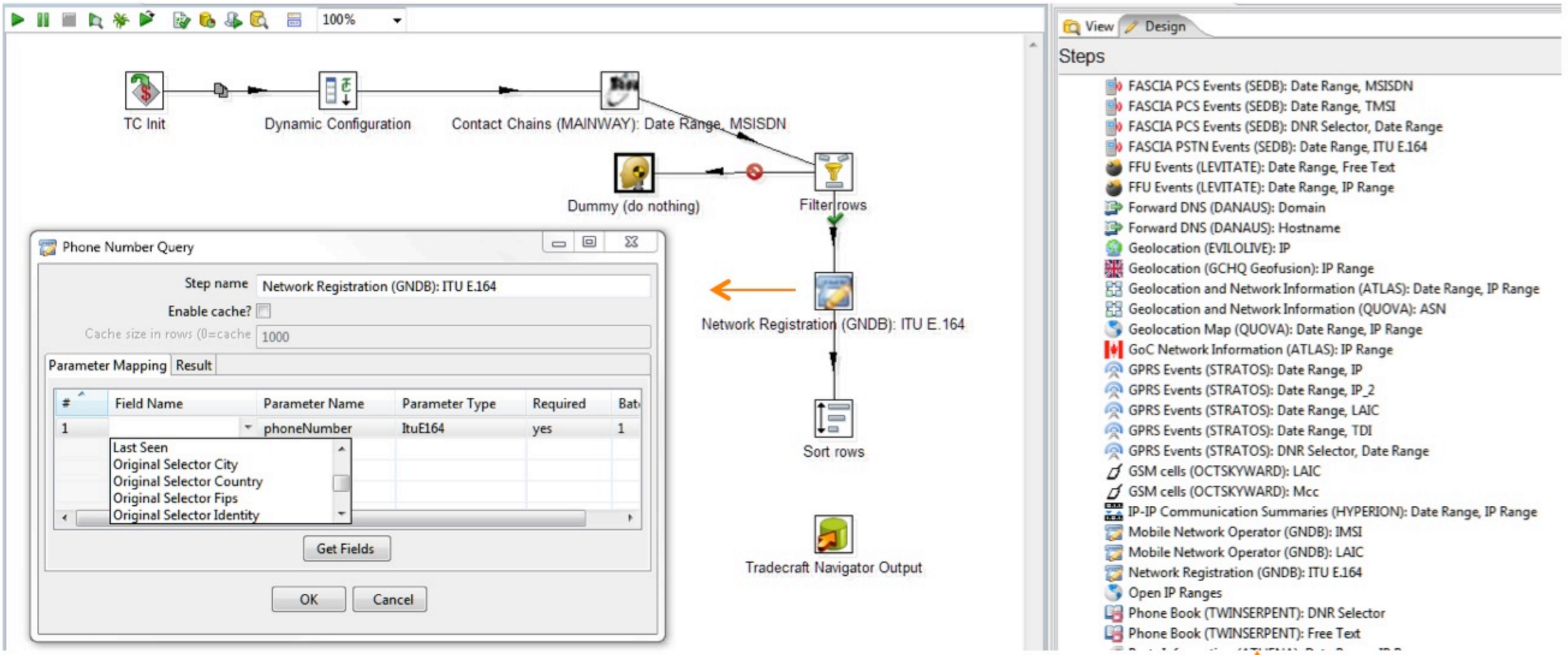
OLYMPIA AT A GLANCE



OLYMPIA AT A GLANCE



OLYMPIA - AUTOMATION



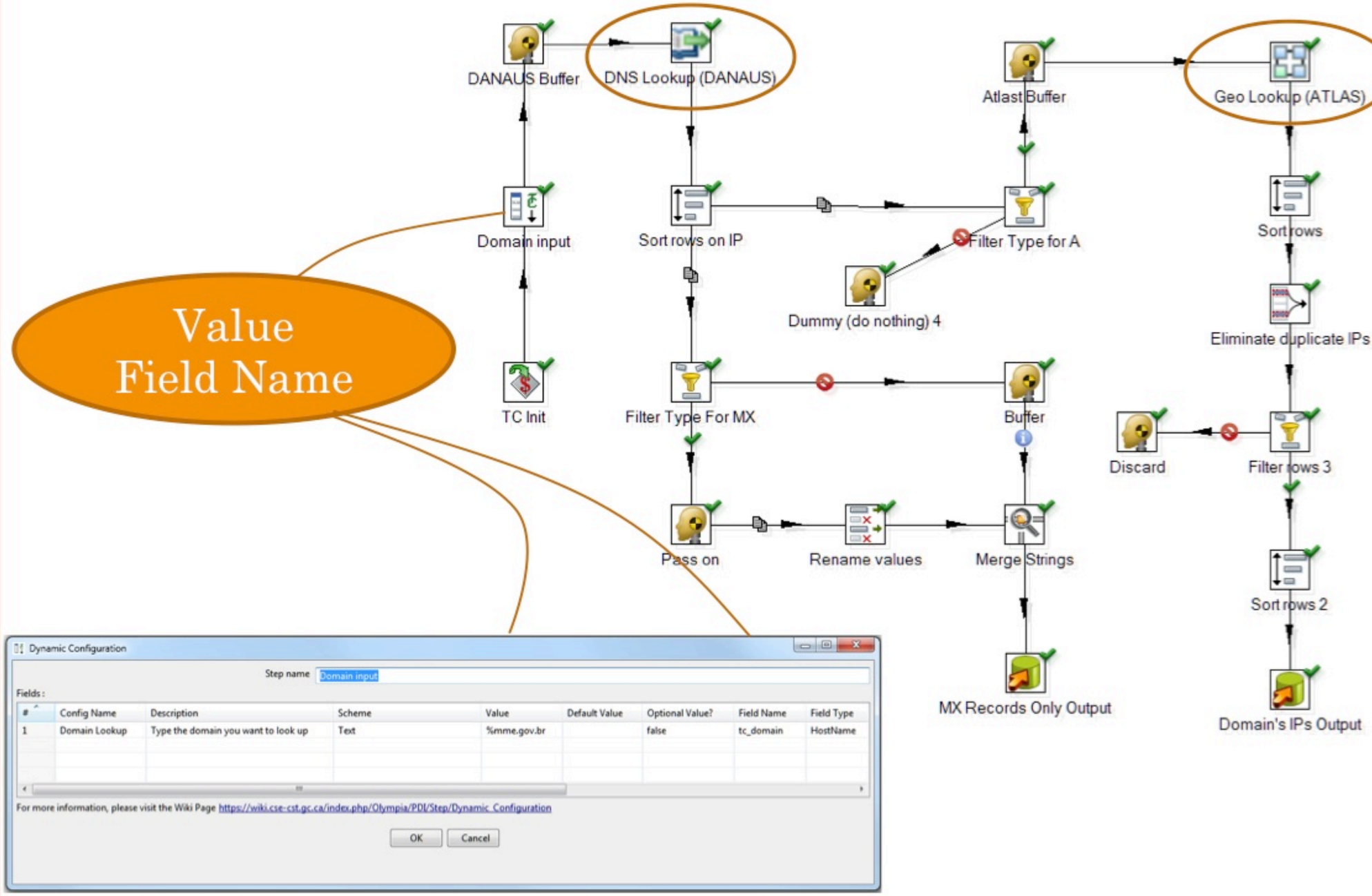
Numerous enrichment and data manipulation nodes
Drag and drop each node
Create links between nodes
Hit the *Play* button

ANALYSIS – CASE STUDY

What we know about the target:

- Domain: @mme.gov.br
- 9 DNR selectors
- Very little collection

ANALYSIS – DETERMINE TARGET'S IPs AND ISPs



ANALYSIS – DETERMINE TARGET'S IPs AND ISPs

Mail Servers Output

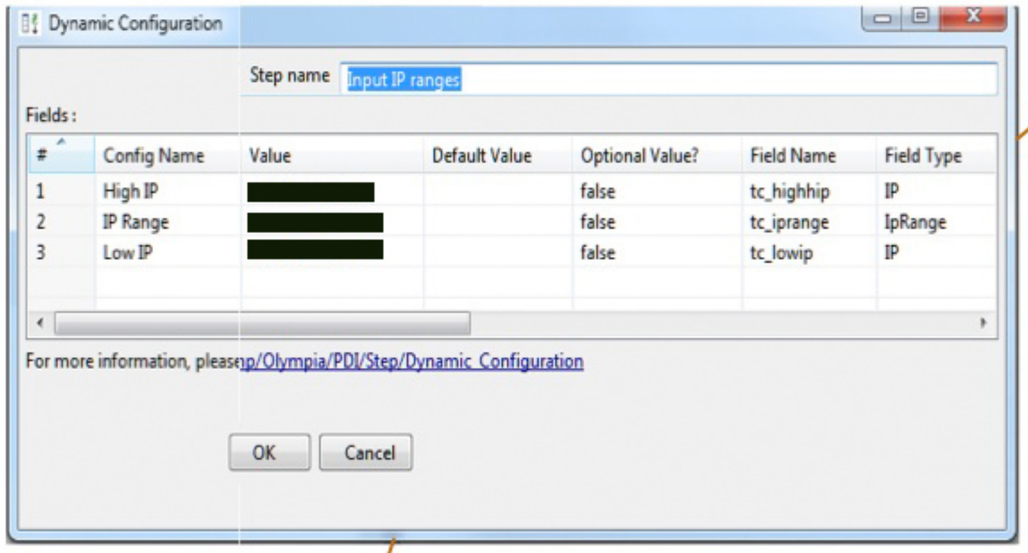
Response_MX	Hostname	IPv4	Source	First Seen	Last Seen
correio.mme.gov.br	correio.mme.gov.br	[redacted]	EONBLUE	Wed Jun 17 06:04:23 GMT 2009	Mon Feb 15 12:40:53 GMT 2010
correio2.mme.gov.br	correio2.mme.gov.br	[redacted]	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011

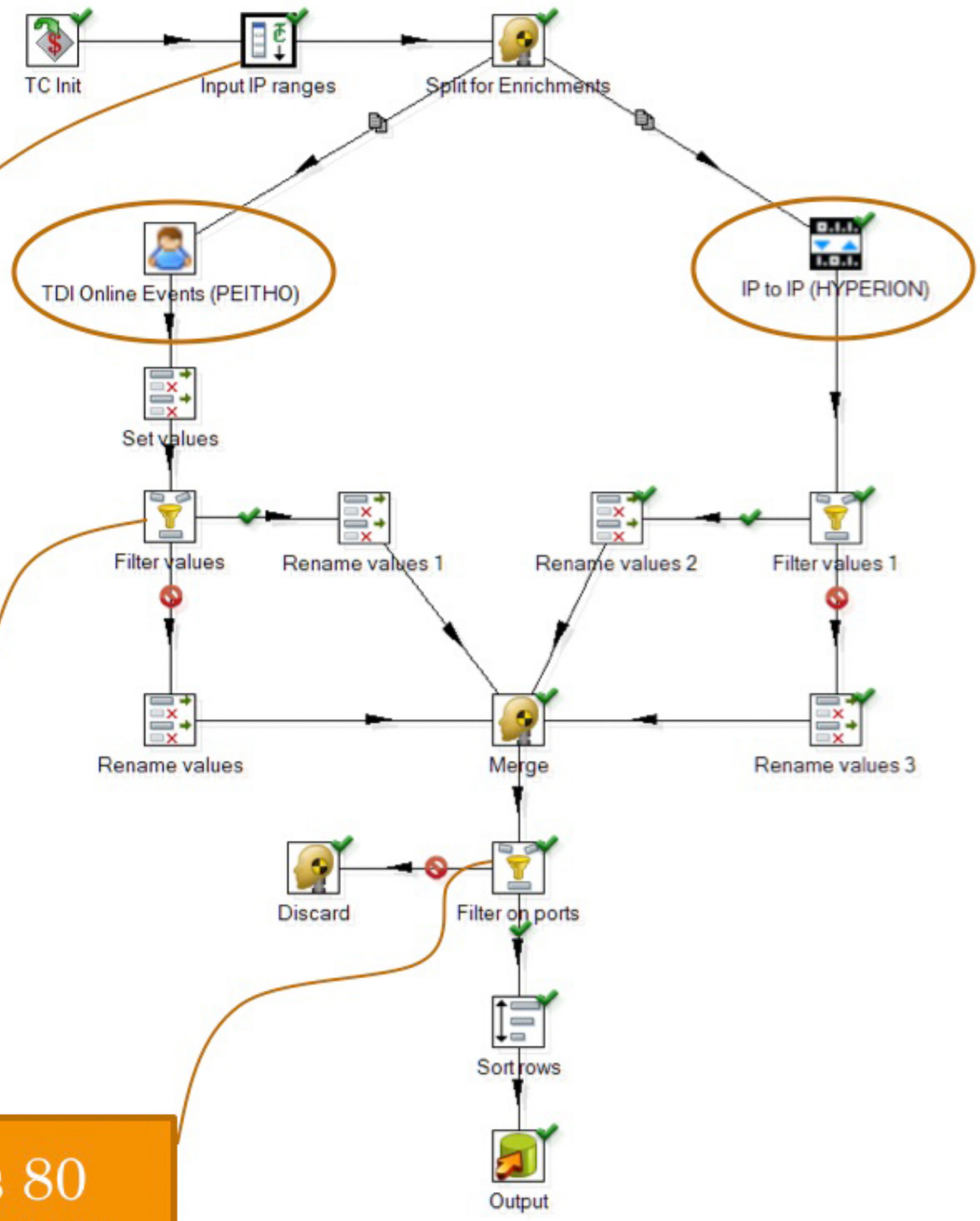
Hostname
IPv4
Country
ASN
Owner
Carrier

Domain's IPs Output

Type	Hostname	IPv4	IP Range	Country	ASN	Owner	Carrier	Source	First Seen	Last Seen
A	ns1.mme.gov.br	[redacted]	[redacted]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Tue May 08 17:28:22 GMT 2012
A	www.mme.gov.br	[redacted]	[redacted]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 22:09:58 GMT 2011	Sat May 05 18:35:50 GMT 2012
A	ns2.mme.gov.br	[redacted]	[redacted]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Tue May 08 17:28:22 GMT 2012
A	srv041.mme.gov.br	[redacted]	[redacted]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Wed Apr 25 04:55:02 GMT 2012
A	correio.mme.gov.br	[redacted]	[redacted]	brazil	18881	comite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 16:26:42 GMT 2011	Wed May 02 21:11:17 GMT 2012
A	acessovpn.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	ns1.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	correio2.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	www.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Thu Feb 11 19:15:47 GMT 2010	Mon Dec 19 19:40:43 GMT 2011
A	ns2.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Wed Sep 15 23:11:59 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	srv041.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Thu Mar 03 19:37:08 GMT 2011	Tue Dec 20 15:49:18 GMT 2011
A	prodeem.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	srv041.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Wed Feb 10 12:51:14 GMT 2010	Tue Sep 07 09:24:15 GMT 2010
A	correio.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Fri Feb 12 20:14:21 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	catalago.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	correio.mme.gov.br	[redacted]	[redacted]	brazil	10954	comite gestor da internet no brasil	serpro	QUOVA	Thu Feb 19 20:37:34 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	correiomme.mme.gov.br	[redacted]	[redacted]	brazil	10954	comite gestor da internet no brasil	serpro	QUOVA	Fri Mar 27 14:03:47 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	urano.mme.gov.br	[redacted]	[redacted]	brazil	10954	comite gestor da internet no brasil	serpro	QUOVA	Fri Mar 27 14:04:08 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	terra.mme.gov.br	[redacted]	[redacted]	brazil	10954	comite gestor da internet no brasil	serpro	QUOVA	Fri Mar 27 14:04:08 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	www.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	catalago.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	webpac.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	prodeem.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	urano.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	terra.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Apr 20 11:12:46 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	correio.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	acessovpn.mme.gov.br	[redacted]	[redacted]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011

ANALYSIS – DISCOVER TARGET'S PROXY





High IP

Low IP

IP Range

REMOTE PORT contains 80
REMOTE PORT contains 443

ANALYSIS – DISCOVER TARGET'S PROXY

Entity IP :

[redacted]

Remote IP : various

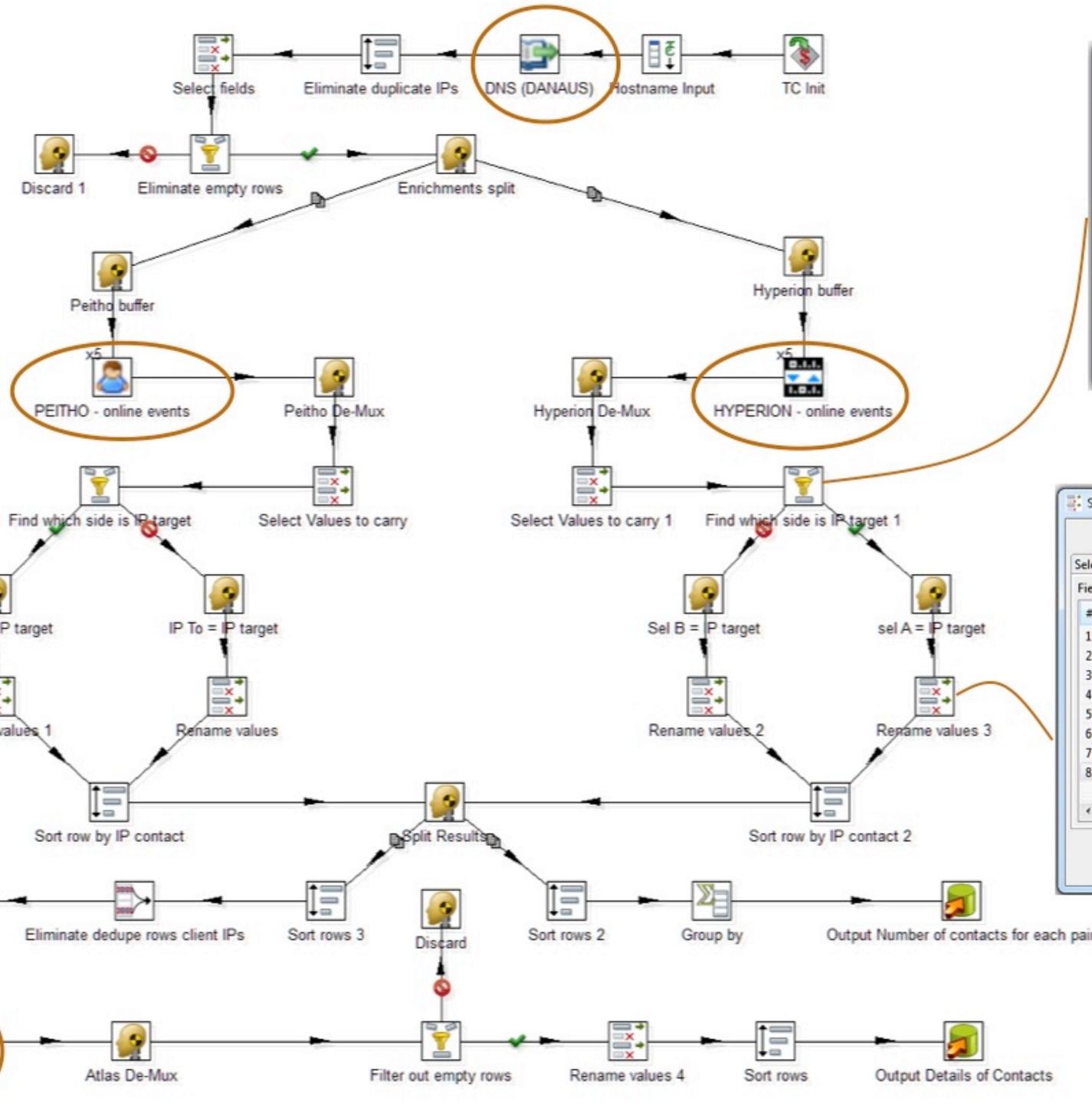
Remote Port : 443

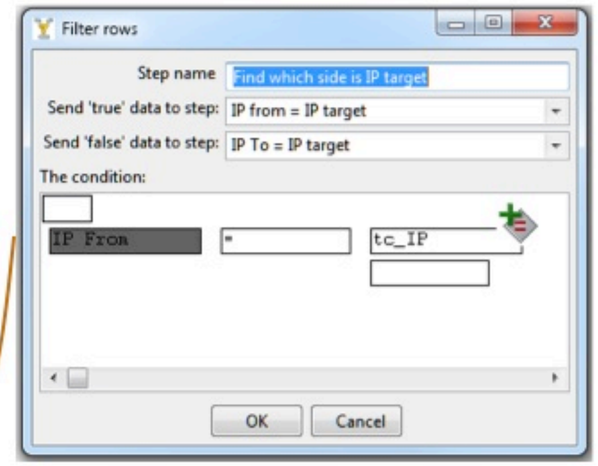
Entity Port: various

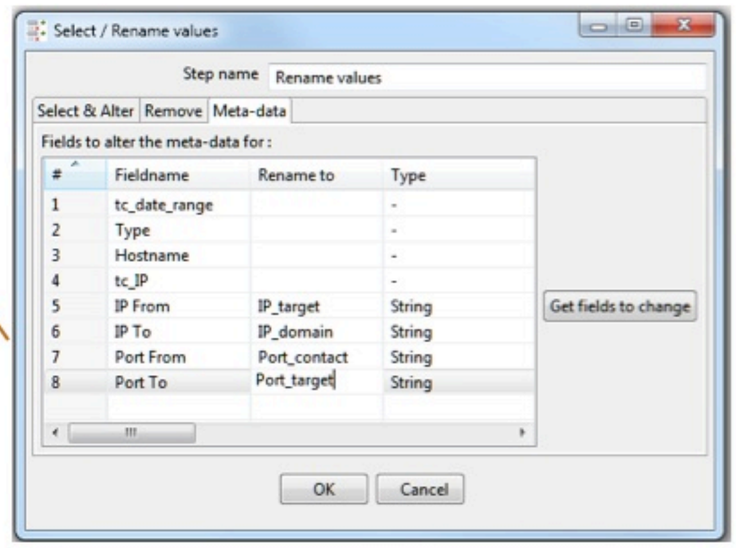
Target Proxy Output

entity_IP	remote_IP	remote_port	entity_port
[redacted]	[redacted]	6:443:TS (1);	6:47367:FC (1);
[redacted]	[redacted]	6:443:TS (1);	6:27973:FC (1);
[redacted]	[redacted]	6:443:TS (1);	6:48329:FC (1);
[redacted]	[redacted]	6:443:TS (2);	6:47950:FC (1);6:483
[redacted]	[redacted]	6:443:TS (2);	6:54695:FC (1);6:435
[redacted]	[redacted]	6:443:TS (4);	6:31670:FC (1);6:343
[redacted]	[redacted]	6:443:TS (5);	6:1263:FC (1);6:4115
[redacted]	[redacted]	6:443:FS (12);	6:48927:TC (1);6:489
[redacted]	[redacted]	6:443:TS (179);6:80:T	6:26704:FC (1);6:267
[redacted]	[redacted]	6:443:TS (1);	6:11217:FC (1);
[redacted]	[redacted]	6:443:TS (165);	6:12946:FC (1);6:152
[redacted]	[redacted]	6:443:TS (1);	6:60657:FC (1);
[redacted]	[redacted]	6:443:TS (1);	6:45811:FC (1);
[redacted]	[redacted]	6:443:TS (14);6:80:TS	6:19170:FC (2);6:536

ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH







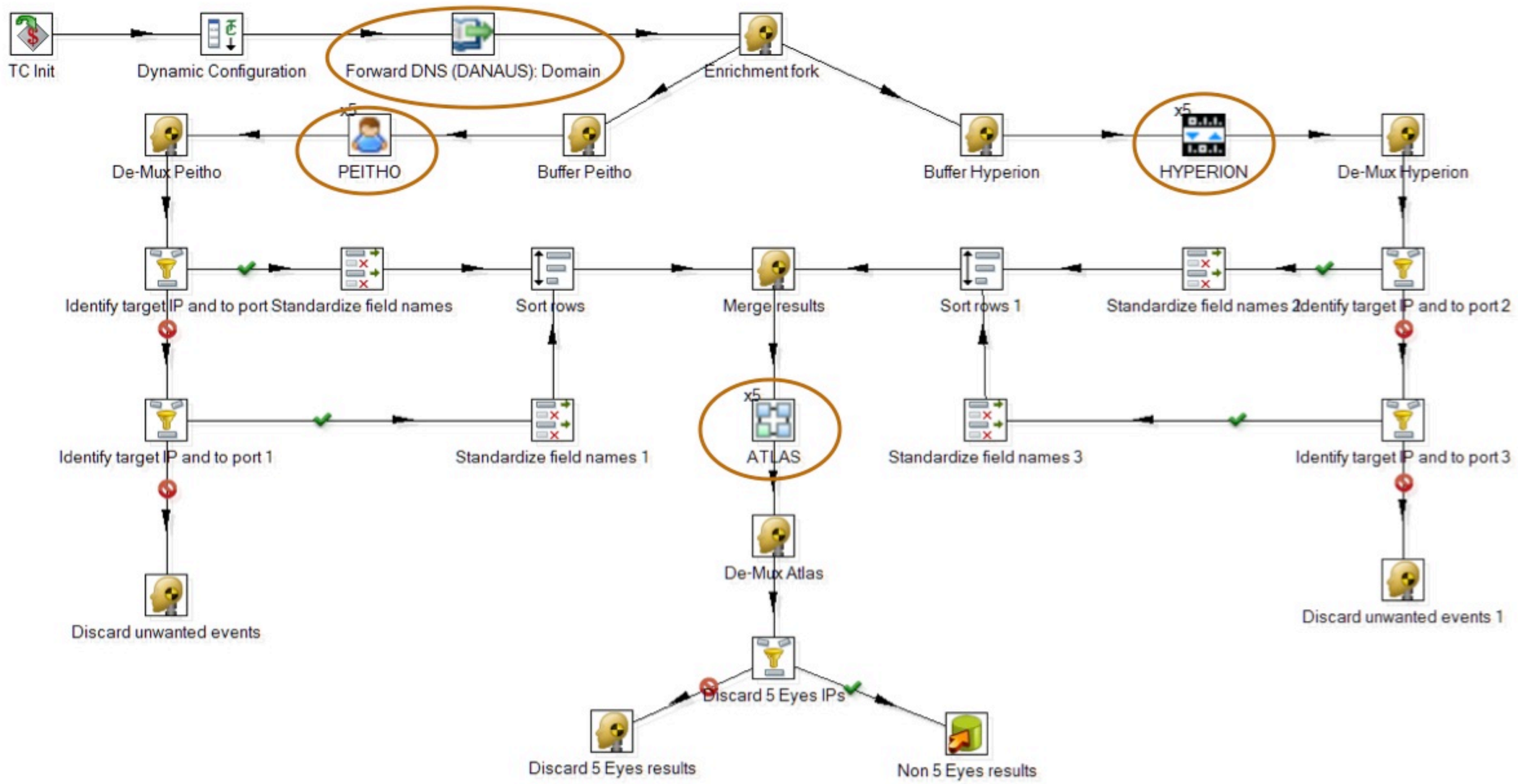
ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH

Hostname domain	IP domain	IP in contact with domain	Port used by IP domain	Port used by IP contact	Owner of IP rcontact	Carrier of IP contact	ASN of IP contact	Country of IP contact	IP range for IP contact
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:61991:FC (1);	tse i net noc ip infrastrcture	british telecommunications plc	5400	eritrea	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:63181:FC (1);	tse i net noc ip infrastrcture	british telecommunications plc	5400	eritrea	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (2);6:25:FS (1);	6:34291:FC (2)	tata communications	tata communications	6453	canada	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:28151:FC (1);	jtc	jordan telecommunications com	8697	jordan	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:2990:FC (1);	reassign to idc-cbw-idc custome	cs loxinfo public company limite	9891	thailand	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:FS (1);	6:50072:TC (1);	internal network	international data exchange llc	12524	jordan	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:51934:FC (1);	pars online	parsonline	16322	iran	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:2295:FC (1);	dsl home subscribers	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:1799:FC (1);	dsl home subscribers	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:50329:FC (1);	dsl home subscribers	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (1);	6:22423:FC (1);	saudinet saudi telecom compan	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:54596:TC	6:25:FS (128);	iweb dedicated hd	iweb technologies inc.	32613	canada	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:33907:TC	6:25:FS (22);	iweb dedicated hd	iweb technologies inc.	32613	canada	[redacted]
correio.mme.gov.br	[redacted]	[redacted]	6:25:TS (4);	6:57773:FC	middle east internet company li	cyberia riyadh	34397	saudi arabia	[redacted]
www.mme.gov.br	[redacted]	[redacted]	6:80:FS (1);	6:54791:TC (1);	adsl service	sahara net	41176	saudi arabia	[redacted]

Hostname starting domain
IP starting domain
IP in contact with starting domain
Port used by starting domain
Port used by IP contact

Owner of IP contact
Carrier of IP contact
ASN of IP contact
Country of IP contact
IP range for IP contact

ANALYSIS – IDENTIFY POTENTIAL MAN ON THE SIDE OPERATION AGAINST MY TARGET



ANALYSIS – IDENTIFY POTENTIAL MAN ON THE SIDE OPERATION AGAINST MY TARGET

Results

target_hostname	target	contact	target_port	contact_port	Case Notations	Country	Digraph
acessovpn.mme.gov.br	[redacted]	[redacted]	6:41278:TC (1);	6:80:FS (1);	MA10099 (1);	brazil	br
acessovpn.mme.gov.br	[redacted]	[redacted]	6:30141:TC (1);	6:80:FS (1);	MA10099 (1);	brazil	br

[redacted]

ASN contact	Country contact	# IPs contact
18881	brazil	26
7738	brazil	11
26599	brazil	6
19182	brazil	3
10429	brazil	2
27717	brazil	2
53006	brazil	2
14080	colombia	1
16735	brazil	1
32613	brazil	1
52972	brazil	1
8151	mexico	1

[redacted]

ASN contact	Country contact	# IPs contact
18881	brazil	15
26599	brazil	9
10429	brazil	7
16735	brazil	5
18479	brazil	3
45774	india	3
7738	brazil	3
19182	brazil	2
27699	brazil	2
13878	brazil	1
14080	colombia	1
16509	brazil	1
17379	brazil	1
28311	brazil	1
28670	brazil	1
32613	brazil	1
4808	china	1
53018	brazil	1
53070	brazil	1
9829	india	1

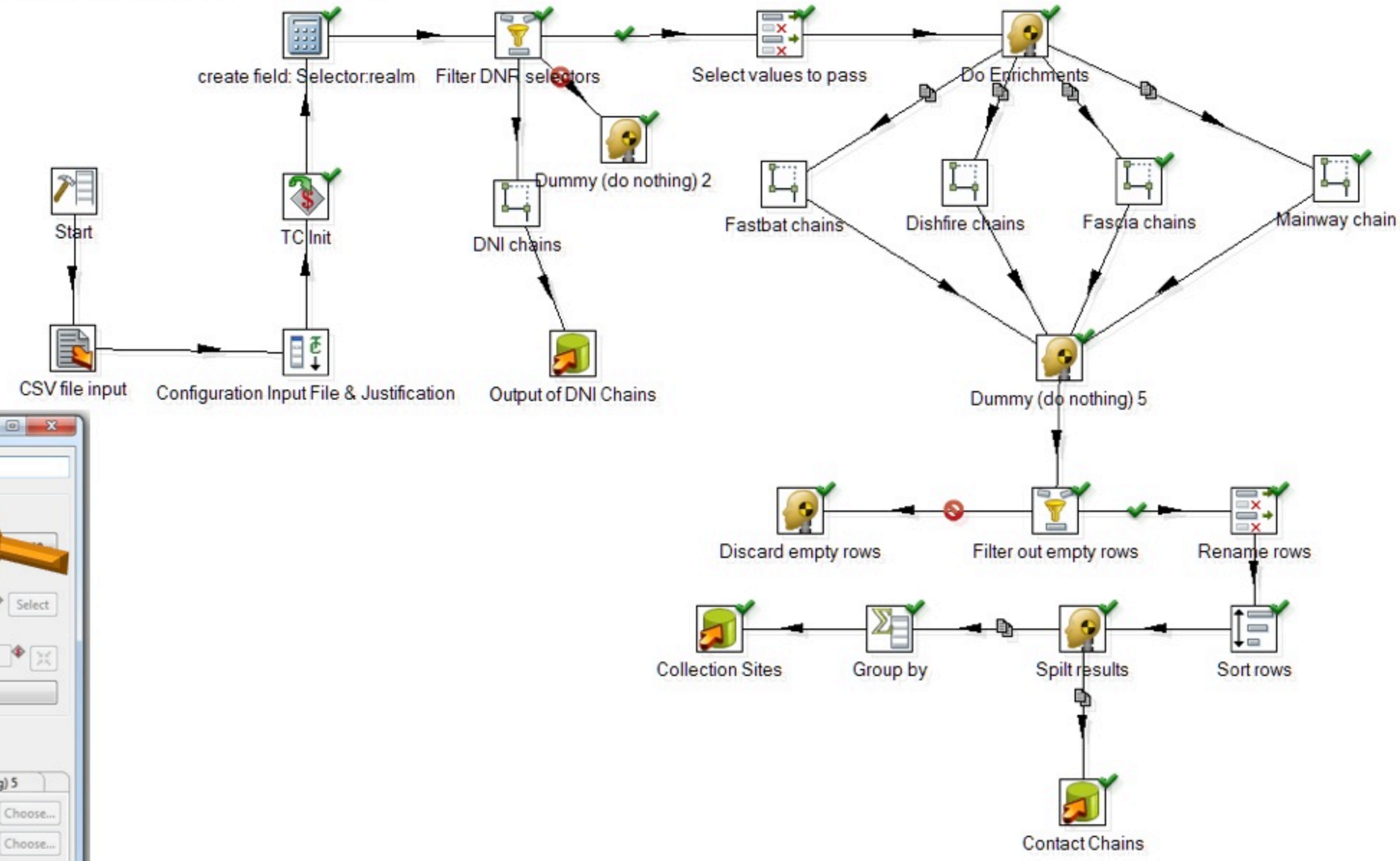
[redacted]

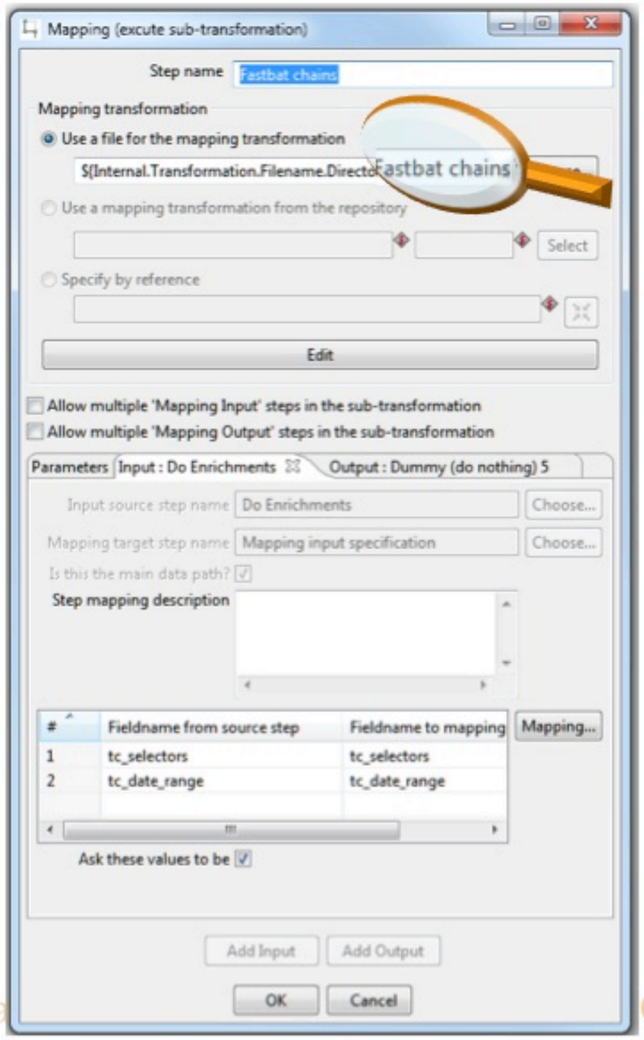
Reverse DNS (DANAUS) for IP (218)

IP = 189.91.32.13

Source	Type	Hostname	Hostname Decoded	IPv4
EONBLUE	A	wcenter.net.br	wcenter.net.br	[redacted]
EONBLUE	A	olaughlin.com.br	olaughlin.com.br	[redacted]
EONBLUE	A	transformadoresuniao.com.br	transformadoresuniao.com.br	[redacted]
EONBLUE	A	geosfera.tur.br	geosfera.tur.br	[redacted]
EONBLUE	A	molybras.com.br	molybras.com.br	[redacted]
EONBLUE	A	fatecitaqua.edu.br	fatecitaqua.edu.br	[redacted]
EONBLUE	A	abiclor.com.br	abiclor.com.br	[redacted]
EONBLUE	A	helendrexel.org.br	helendrexel.org.br	[redacted]
EONBLUE	A	afabbsp.com.br	afabbsp.com.br	[redacted]
EONBLUE	A	advocc.com.br	advocc.com.br	[redacted]
EONBLUE	A	metaljato.com.br	metaljato.com.br	[redacted]
EONBLUE	A	guriastore.com.br	guriastore.com.br	[redacted]
EONBLUE	A	ateq.com.br	ateq.com.br	[redacted]
EONBLUE	A	flatexpress.com.br	flatexpress.com.br	[redacted]
EONBLUE	A	mhrviagens.com.br	mhrviagens.com.br	[redacted]
EONBLUE	A	stephandoit.com.br	stephandoit.com.br	[redacted]
EONBLUE	A	2houseimoveis.com.br	2houseimoveis.com.br	[redacted]
EONBLUE	A	thats.com.br	thats.com.br	[redacted]
EONBLUE	A	galina.com.br	galina.com.br	[redacted]
EONBLUE	A	edpcrh.com.br	edpcrh.com.br	[redacted]
EONBLUE	A	institutodopvc.org	institutodopvc.org	[redacted]

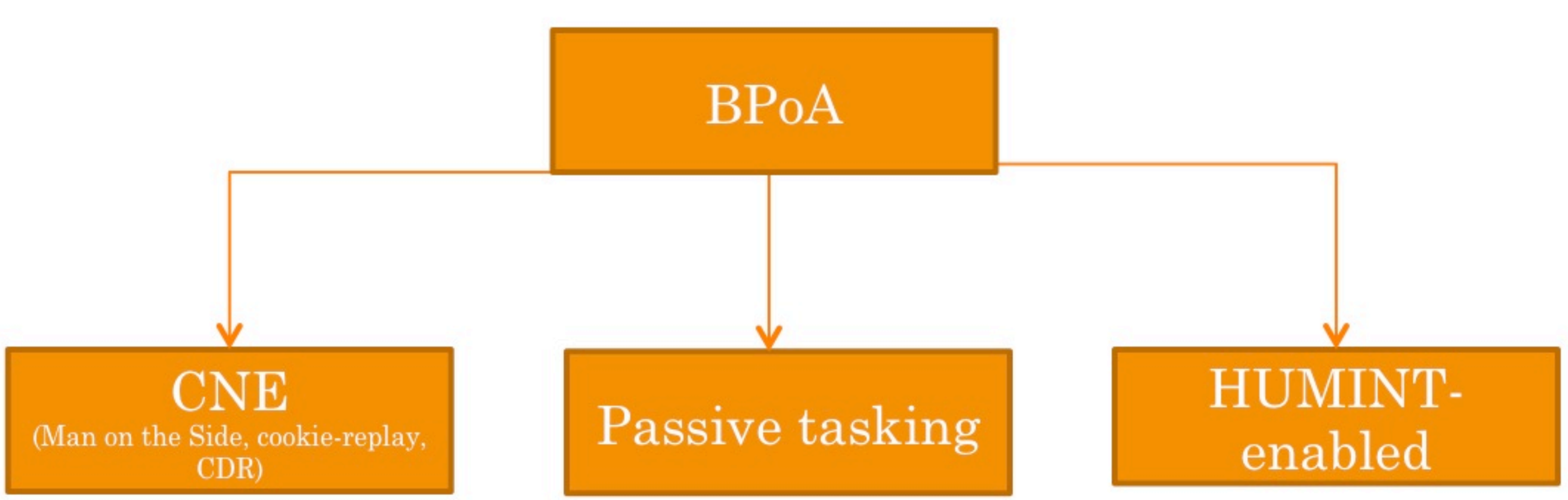
ANALYSIS – DISCOVER CONTACTS OF MY TARGET AND COLLECTION SITES I SEE MY TARGET ON





SUMMARY

Based on the information collected, I am better positioned to analyse my target's telecoms environment.



MOVING FORWARD

- I have identified MX servers which have been targeted to passive collection by the Intel analysts, who are assessing the value, provenance, etc. of the traffic generated by the mail servers.

- I am working with TAO to further examine the possibility for a Man on the Side operation.

- Based on the network information gathered, the NAC has started a BPoA analysis on the MME.