

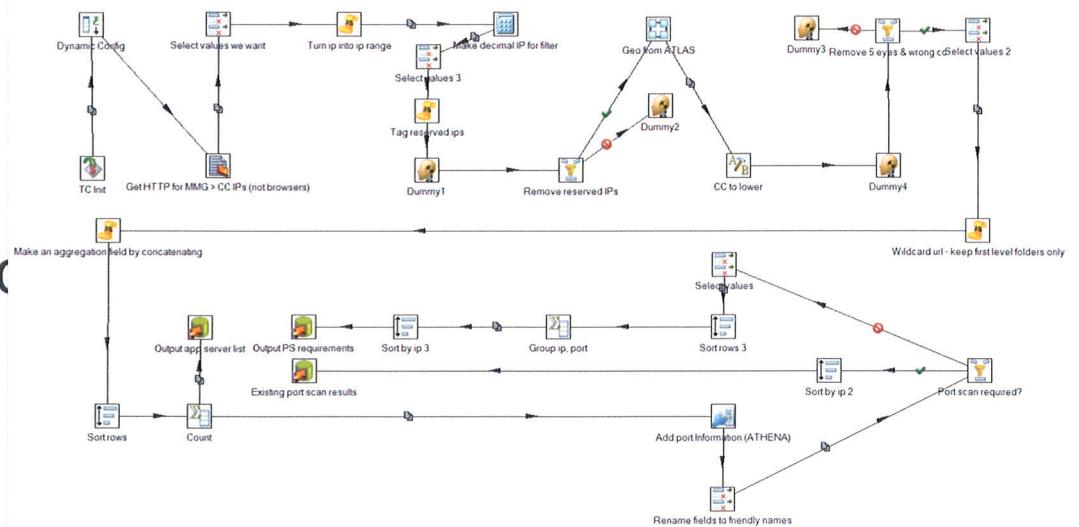
# Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team  
(NTAT)



# Overview

- \* What is the NTAT?
- \* 2011 – 2012 work and accomplishments



TOP SECRET//SI



# Tradecraft?

## Tradecraft

- “The development of methods, techniques, algorithms and processes in order to generate Intelligence, and developing the ability to apply this knowledge either manually or through automation. Tradecraft is developed from experience, research, intuition and by the reapplication and redefinition of existing techniques. **Industrial-Scale Tradecraft** involves data on a large scale.”

## Network Tradecraft

- Usable knowledge about how to acquire intelligence FROM the network

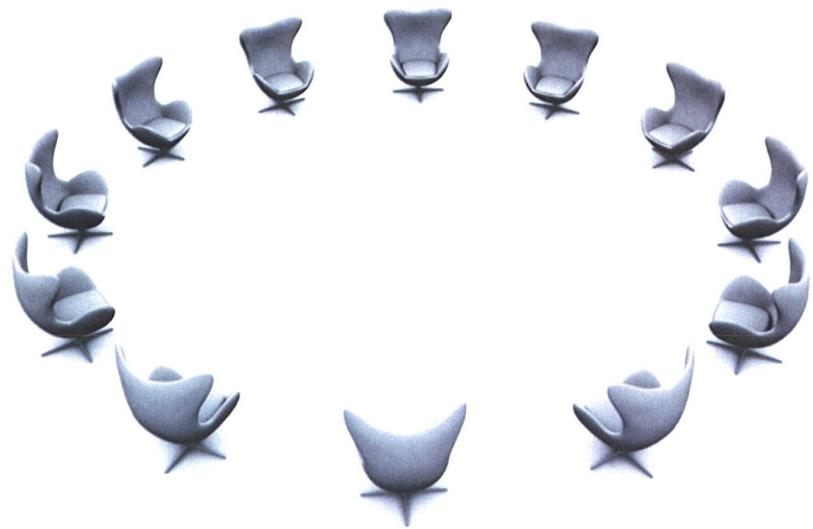


TOP SECRET//SI



# The NTAT

- \* Create repeatable,  
sustainable & shareable  
tradecraft to enable  
network analysis
- \* Facilitate knowledge  
collaboration and  
interchange across the 5-  
Eyes SIGDEV community



TOP SECRET//SI



# The Process

**Stage 1 = Fact Finding**

**Stage 2 = Define Focus (based on Fact Finding)**

**Stage 3 = Develop Tradecraft**

**Stage 4 = Document Tradecraft**

**Stage 5 = Test Documented Tradecraft and Refine**

TOP SECRET//SI



# Network Convergence Tradecraft

- \* Technological convergence – where voice and data services interact with each other on a single device
- \* Tradecraft to enable the targeting of handsets in telephony space and CNE exploitation in IP space
- \* Improved algorithms for mobile gateway identification and implementation of these algorithms



TOP SECRET//SI



# DSD Workshop

## November 2011

- \* 2 weeks
  - \* CSE, DSD, GCHQ
  - \* Virtually, via chat room, NSA & GCSB
- \* Focus on data, techniques & analytic outcomes

<https://wiki.dsdp/twiki/>



# DSD Workshop Outcomes

Technique developed to identify wide variety of potential converged data, unique for specific country or mobile network operator

- Ø ***potentially lead to convergence correlation dataset to help profile targets on-line activity***

Documentation of techniques to identify specific components of raw HTTP activity that alludes to the browsing, downloading and installation of smartphone applications

- Ø ***identified the presence of application servers for mobile network operators and geographical areas***

DSD implementation of mobile gateway identification analytic based on FRETTING YETI

- Ø ***three agencies now running the same analytic provides a richer dataset of mobile gateways***

CRAFTY SHACK trial

- Ø ***NTAT now using CRAFTY SHACK for tradecraft documentation***



# XKS Microplugin: Samsung Protocol

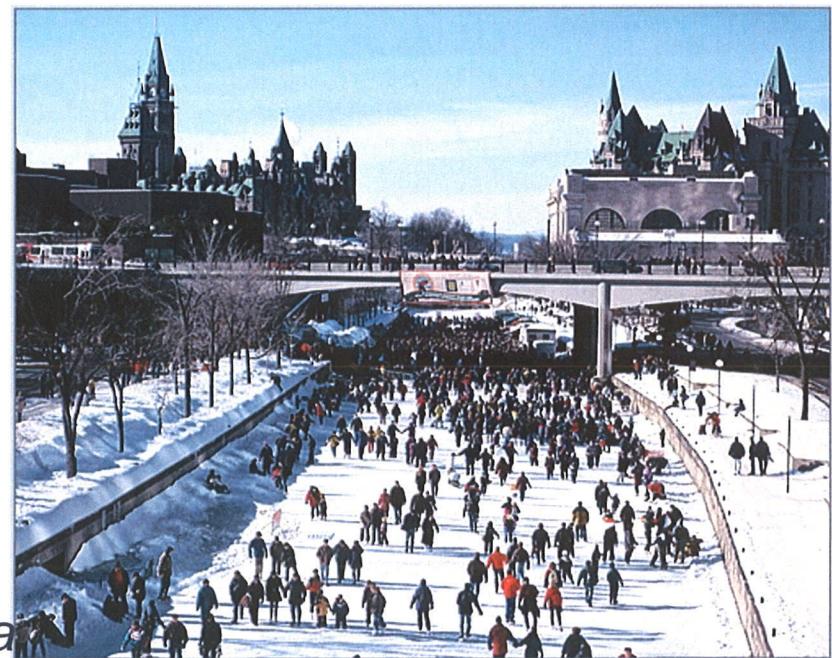
1		1	1	CSC	Device_Model	HTTP_User_Agent	Imei	Latest_Mcc	Mcc	Message_Id	Message_Type	Mnc	Network_Ty	Odc_Versio	loaded_Postloaded_e_Preload	
2		1	1	352	T-KSA	GT-N7000	SAMSUNG-Android		412	2306-8	checkAppUpgrade Request	50	0	2.6.084	com.sec.android.app.samsungapp@2.1.0a	
3		1	1	666	1	AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021	com.sec.android.app.samsungapp 1.0
4		1	1	648	1	AUT	GT-P7500	SAMSUNG-Android		250	2306-1	checkAppUpgrade Request	01	0	3.0.021	com.sec.android.app.samsungapp 1.0
5		1	1	1269	1	AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021	com.sec.android.app.samsungapp 1.0
6		1	1	1281	1	AUT	GT-P7500	SAMSUNG-Android		250	2306-3	checkAppUpgrade Request	01	0	3.0.021	com.sec.android.app.samsungapp 1.0
7		1	1	1262	1	AUT	GT-P7500	SAMSUNG-Android		250	2306-4	checkAppUpgrade Request	01	0	3.0.021	com.sec.android.app.samsungapp 1.0
8		1	1	1274	1	AUT	GT-P7500	SAMSUNG-Android		250	2306-5	checkAppUpgrade Request	01	0	3.0.021	com.sec.android.app.samsungapp 1.0a
9		1	1	1	1	AUT	GT-P7500	SAMSUNG-Android		412	2306-0	checkAppUpgrade Request	20	0	2.6.148	3.0
10		1	1	62	1	SKZ	GT-I9100	SAMSUNG-Android		412	2350-0	getPushNotificationMessage Re	20	0		3.0
11		1	1	433	1	XSG	GT-I9100	SAMSUNG-Android		412	2350-0	getPushNotificationMessage Re	20	0		3.0
12		1	1	463	1	XSG	GT-I9100	SAMSUNG-Android		412	2350-0	getPushNotificationMessage Re	20	0		3.0
13		1	1	1074	1	XSG	GT-I9100	SAMSUNG-Android		412	2309-0	getDownloadList Request	20	0		3.0
14		1	1	788	1	XSG	GT-I9100	SAMSUNG-Android		412	2308-0	getKillList Request	20	0		NFDJ000000M017
15		1	1	1110	1	XSG	GT-I9100	SAMSUNG-Android		412	2301-0	getUpgradeKillCount Request	20	0		3.0
16		1	1	664	1	XSG	GT-I9100	SAMSUNG-Android		412	2301-0	getUpgradeKillCount Request	50	0		E90H000000M000
17		1	1	369	1	XSG	GT-I9100	SAMSUNG-Android		412	2301-0	getUpgradeKillCount Request	50	0		com.sec.android.app.samsungapp 1.0a
18		1	1	362	1	XSG	GT-I9100	SAMSUNG-Android		412	2309-0	getDownloadList Request	50	0		android@2.3.5@0 android.tts@2.3.1.0a
19		1	1	499	1	XEU	GT-I9100	SAMSUNG-Android		412	2306-5	checkAppUpgrade Request	40	0	2.6.122	E90H000000M000
20		1	1	572	1	XEU	GT-I9100	SAMSUNG-Android		412	2302-2	upgradeListEx Request	20	0	2.6.194	com.sec.android.app.samsungapp 1.0a
21		1	1	951	1	XEU	GT-I9100	SAMSUNG-Android		412	2160-6	purchaseDetailEx Request	20	0	2.6.194	E90H000000M000
22		1	1	864	1	THR	GT-B5512	SAMSUNG-Android		412	2306-2	checkAppUpgrade Request	20	0	2.6.048	cn.wps.mc 173
23		1	1	955	1	XSG	GT-I9100	SAMSUNG-Android		412	2300-0	checkAppUpgrade Request	20	0	2.6.048	com.sec.android.app.samsungapp 1.0a
24		1	1	956	1	XSG	GT-I9100	SAMSUNG-Android		412	2300-0	countrySearchEx Request	20	0		E90H000000M000
25		1	1	1259	1	XSG	GT-I9100	SAMSUNG-Android		412	2200-1	countrySearch Request	111			com.sec.android.app.samsungapp 1.0a
26		1	1	1344	1	XSG	GT-I9100	SAMSUNG-Android		412	2200-1	countrySearch Request	111			E90H000000M000
27		1	1	1400	TOP SECRET//SI//IPF	2012-05-11 10:42:51				412	2200-1	countrySearch Request	111			E90H000000M000
28		1	1	54	TOP SECRET//SI//IPF	2012-05-11 06:43:27				412	2300-0	countrySearchEx Request	20	0		3.0
29		1	1	417	TOP SECRET//SI//IPF	2012-05-13 02:32:35				412	2200-1	countrySearch Request	111			1.0
30		1	1	488	TOP SECRET//SI//IPF	2012-05-11 09:32:39				412	5060-1	termInformation Request	20	0	2.6.048	E90H000000M000

TOP SECRET//SI



# CSE Workshop February 2012

- \* 2 weeks
  - \* CSE, DSD, GCHQ, GCSB, NSA – everyone wanted to experience a Canadian winter!
  - \* Build on the work started at DSD



TOP SECRET//SI



# The Reality!



# CSE Workshop Outcomes

Refinement of XKS fingerprints to identify mobile bearers, Samsung and Android Marketplace servers

- ∅ *17 XKS fingerprints deployed*

Documentation of analytics in CRAFTY SHACK

- ∅ *These analytics are now being implemented across the 5 Eyes*

Proving the tradecraft actually works!

- ∅ *Scenario to test the tradecraft and analytics – Op IRRITANT HORN*



# Op IRRITANT HORN



© AP Photo



TOP SECRET//SI

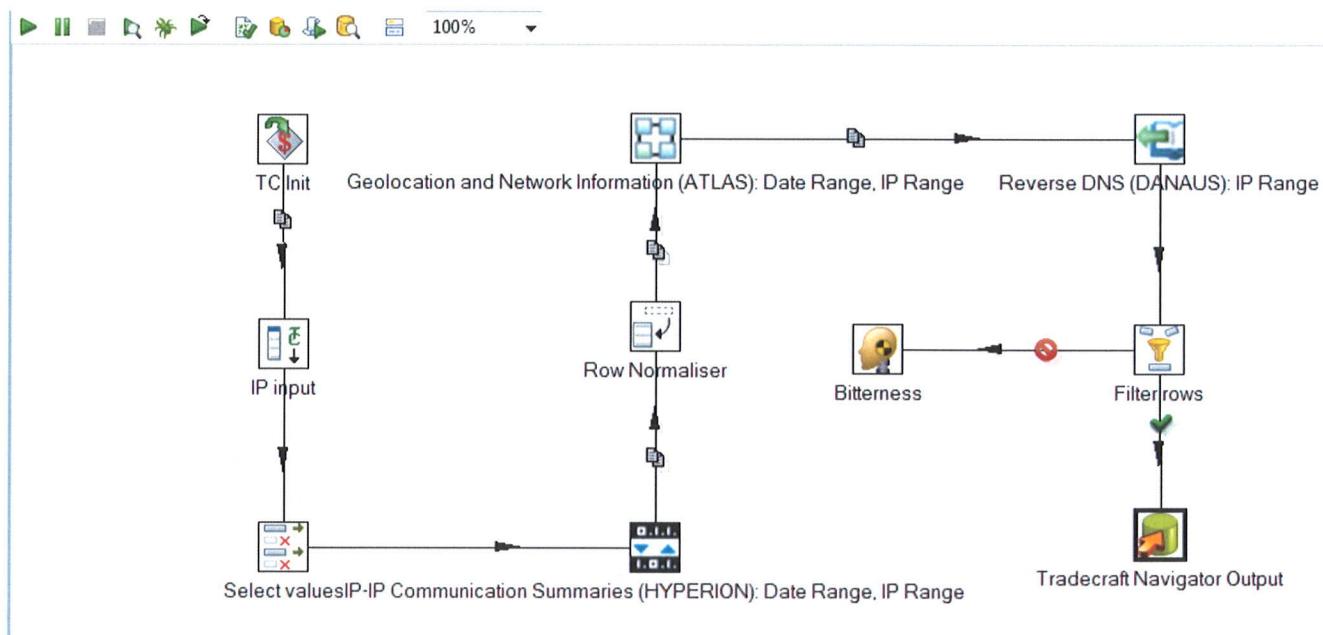
# Op IRRITANT HORN

## Does the tradecraft work?

- \* Another Arab Spring (only this time, different countries)
- \* Goal: identify aggregation points for the mobile networks in the countries of interest using the tradecraft developed during the workshops
- \* Did it work? YES -> the team was able to identify connections from the countries to application and vendor servers in non 5-Eyes countries
- \* So what? We found some servers....
  - Ø Potential MiTM
  - Ø Effects
  - Ø Harvesting data at rest
  - Ø Harvesting data in transit



# Finding mobile application & vendor update servers

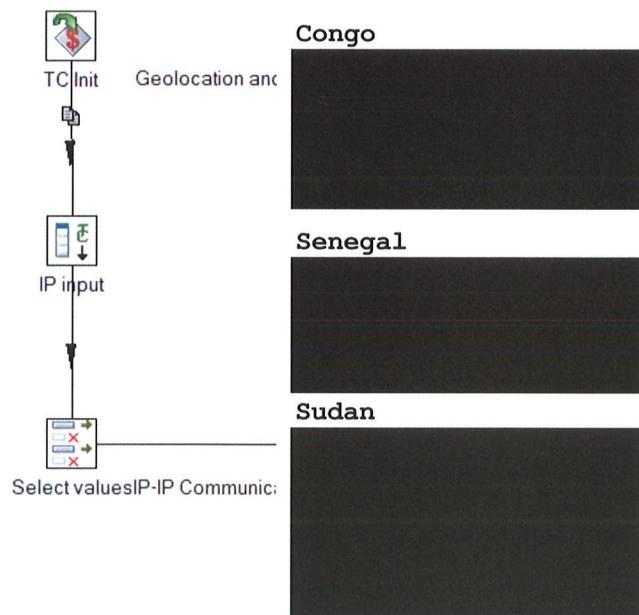


TOP SECRET//SI



# Finding mobile application & vendor update servers

Geolocation analysis



france	android-market.l.google.com
cuba	store.cubava.cu
cuba	store.cubava.cu
senegal	srv_applis.sar.sn
morocco	bounceontelephone.com
switzerland	download-force.com
bahamas	supportapple.com
cuba	store.cubava.cu
netherlands	mobile.ero-advertising.com
russia	lady.marketgid.info

TOP SECRET//SI



Change view [cse-cst.gc.ca]

Search this wiki  Go Search

Crafty Shack

Browse ▾ Search ▾ Create ▾ Help ▾

Identify Servers communicating with a Mobile network

Page Discussion History Edit

**SECRET**

## Identify Servers communicating with a Mobile network

5 EYES CSEC DSD GCHQ GCSB NSA Factbox

Metadata

What does the tradecraft achieve?

- This tradecraft will provide a list of servers that have been seen communicating with a mobile network.

In what situations would this tradecraft be most useful?

- To identify mobile application servers for a specific network
- To identify any server that may be useful for collection purposes

Describe any problems, caveats or things to watch out for

- The list of servers returned depends on the IP range and collection sources utilized. Success of this tradecraft may require additional research to identify other IP ranges or requesting other agencies to check their collection to identify different servers.

Links that can help you to implement this tradecraft

Created by:	[REDACTED]	Difficulty:		Acceptance state:	Limited
Agency:	NSA	Email Address:	[REDACTED]		

**Input(s):** OntologyNetwork block, OntologyIp address    **Output(s):** OntologyIp address, OntologyASN, OntologyNetwork block, OntologyHostname, OntologyUser Agent String, OntologyGeographic selector

**Invokes Tradecraft:**

- Find public IP space used by Mobile Devices and Related Servers on the Internet
- Finding Mobile Internet Gateways

**Input(s):** OntologyNetwork block, OntologyIp address    **Output(s):** OntologyIp address, OntologyASN, OntologyNetwork block, OntologyHostname, OntologyUser Agent String, OntologyGeographic selector

**Invokes Tradecraft:**

- Find public IP space used by Mobile Devices and Related Servers on the Internet
- Finding Mobile Internet Gateways

**Alternatives:**

- Identify Servers communicating with a Mobile network

**5 EYES Tradecraft Steps (document underlying analytic, do not include tools)** [edit]

The IP ranges utilized for the initial implementation of this tradecraft were the Inter PLMN Backbone IP ranges obtained from IR21 documents. For other methods of identifying mobile IP blocks, see the invoked tradecraft listed above.

**Step 1** Take IP ranges or individual addresses identified as being related to mobile network communications.  
**Step 2** Obtain geolocation information and network ownership information for each IP address. This should include Network Owner name, Carrier name, ASN, Continent, Country, Region, City, LatLong, and any other related details that your system can obtain.  
**Step 3** Obtain Internet communication events related to the IP addresses. These events should minimally include source information, To IP, From IP, TCP Direction, and HTTP User-Agent.  
**Step 4** Sort the results and dedup them. This step depends on your collection sources.  
**Step 5** Filter out server communications that have user-agents that aren't useful. Further analysis is needed to identify the non-useful user-agents (cheat sheet needed). Ex friendly-scanner  
**Step 6** Check the TCP Direction field

- If Server to Client, grab the From IP information
- If Client to Server, grab the To IP information
- If Server to Server, grab both the To and From IP information
- If Unknown, capture in an error log

**Step 7** Sort and dedup again based on Server IP information. TCP Direction info is no longer needed.  
**Step 8** Obtain geolocation information and network ownership information for each Server IP. This is done for the servers that were not in the original IP blocks.  
**Step 9** Remove any servers that are not useful. This may include 5-Eyes servers.  
**Step 10** Output

- List of Servers
- List of related User Agents
- List of related hostnames

Average article quality based on 1 rating(s)

Last updated 24/2/2012 by [REDACTED]

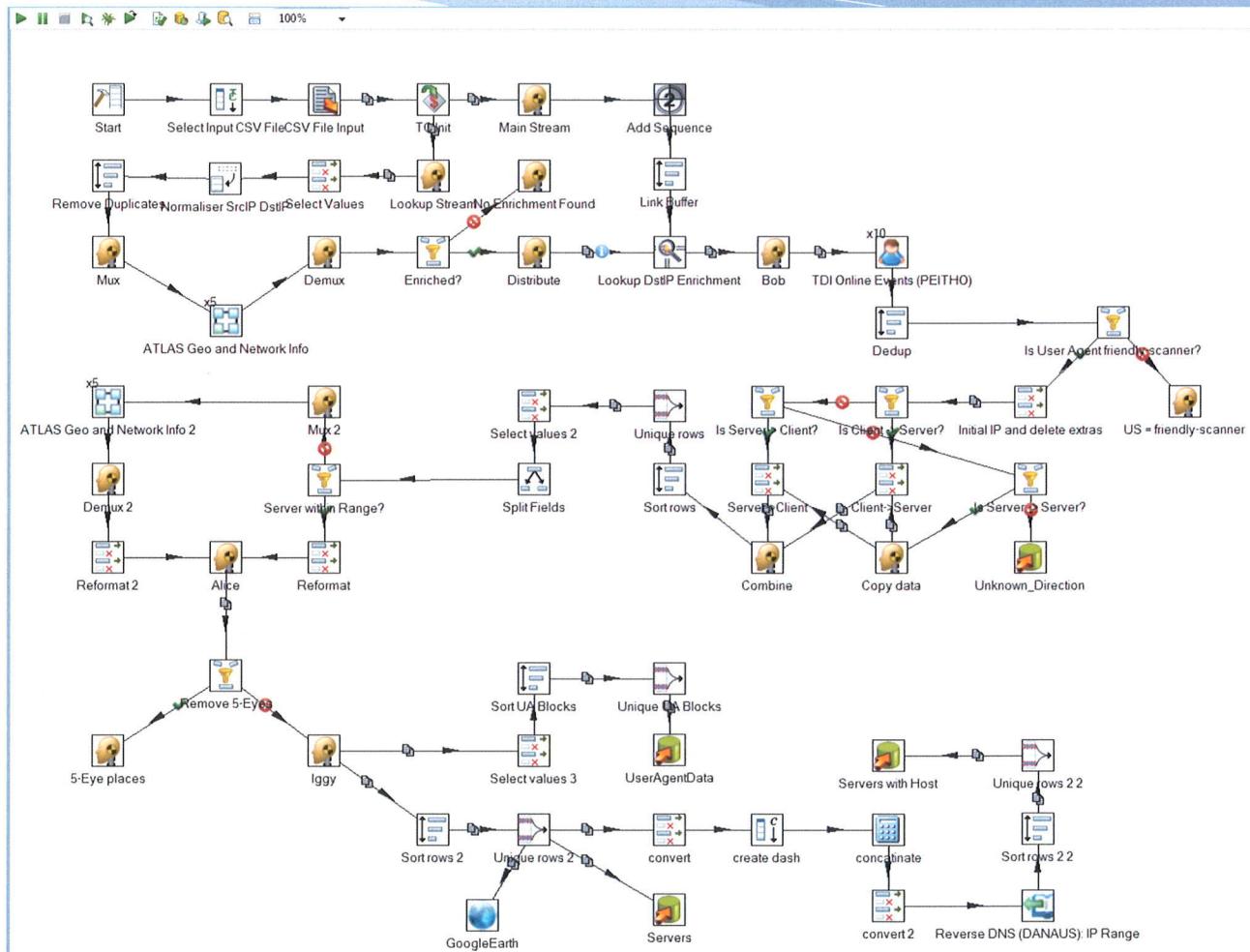
Category: Tradecraft

CRAFTY SHACK - "It's not tradecraft until it's documented!" - CSEC [edit]

TOP SECRET//SI



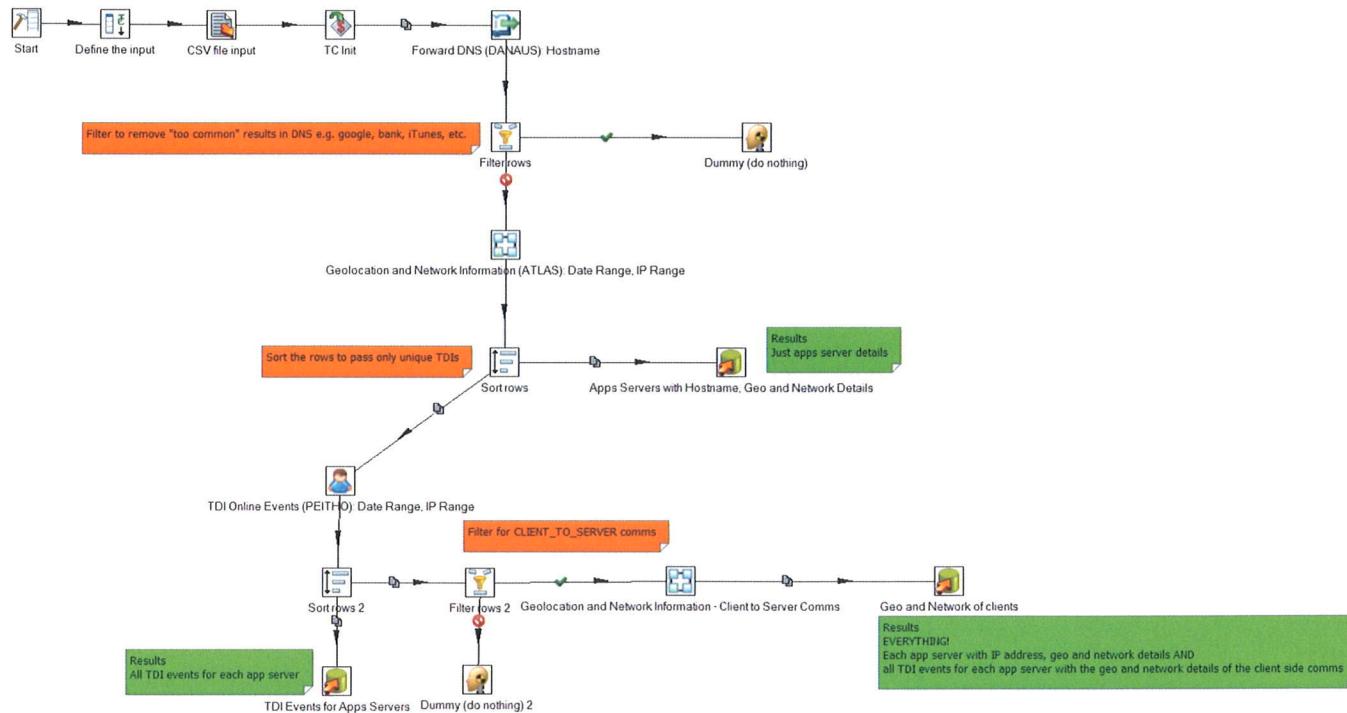
# Identifying servers communicating with an MNO



TOP SECRET//SI

# Profiling mobile application servers

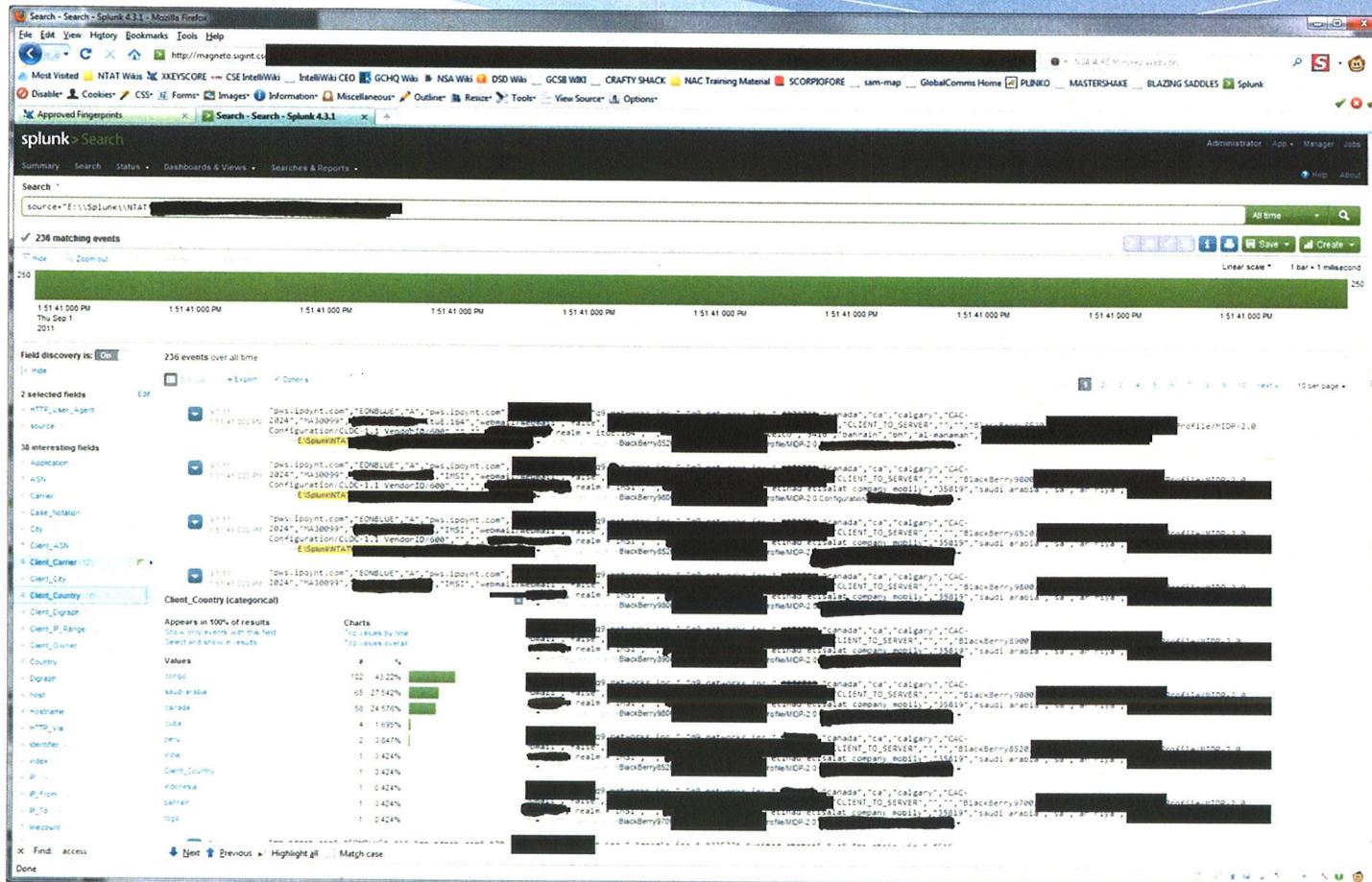
This tradecraft will accept a CSV file of known apps server hostnames. It will then perform reverse DNS queries to obtain the IP addresses of the apps servers. With the IP addresses, geolocation and network provider queries will be performed on all app server IP addresses. The IP addresses are then used to search for TDI events associated with those IP addresses. The result is a list of the apps servers with IP addresses, geolocation and provider details, as well as TDI events seen connecting to those apps servers. The TDI events are also queried to determine their geolocation and provider details.



TOP SECRET//SI



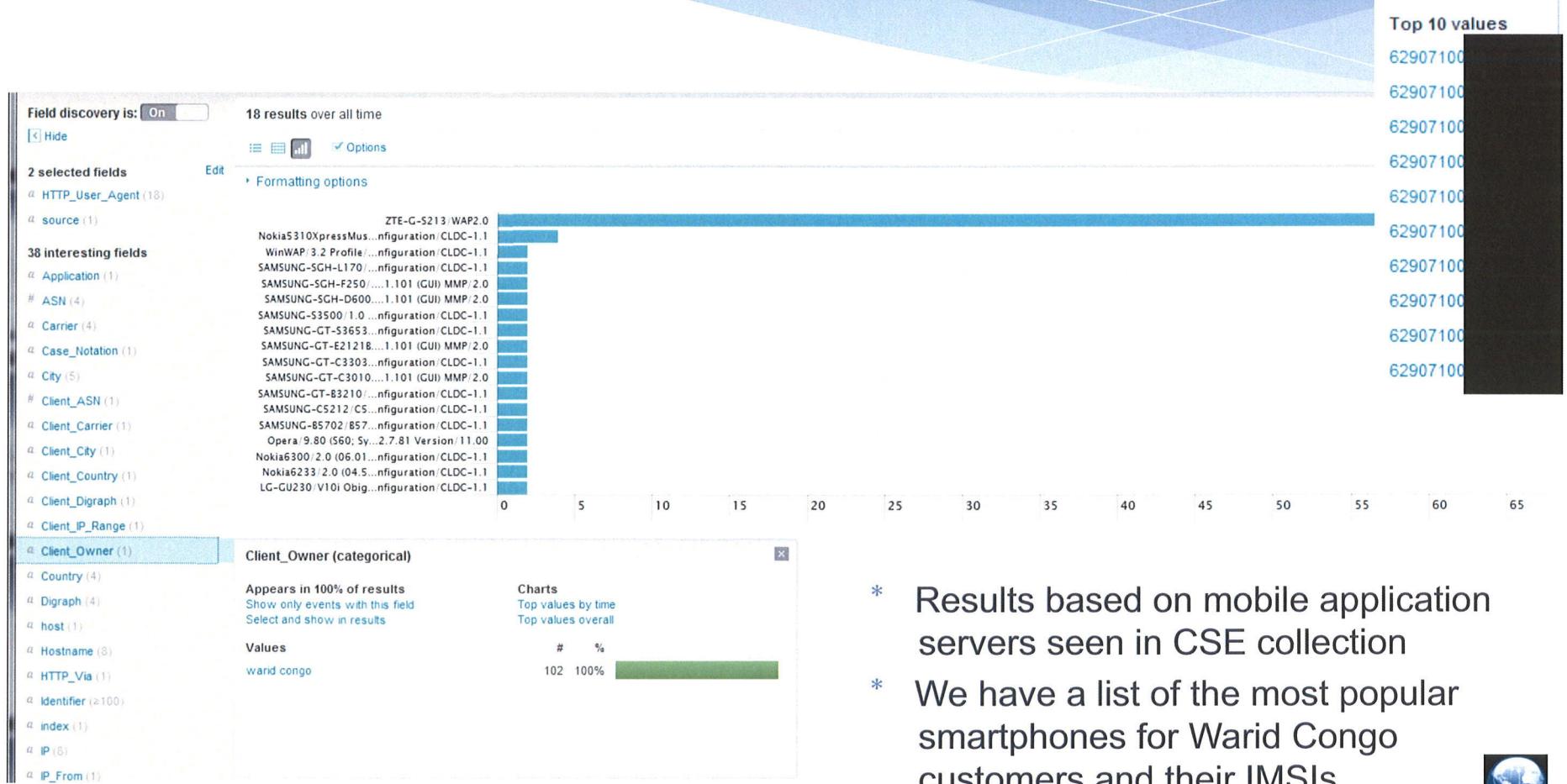
# Profiling mobile application servers



TOP SECRET//SI



# Profiling mobile application servers



- \* Results based on mobile application servers seen in CSE collection
- \* We have a list of the most popular smartphones for Warid Congo customers and their IMSIs



TOP SECRET//SI

# Success Stories

- \* UCWeb mobile browser identification
  - \* Discovered by GCHQ analyst during DSD workshop
- \* Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics



# UCWeb

- \* Led to discovery of active comms channel from [REDACTED]

(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [REDACTED] that is associated with the [REDACTED]

[REDACTED] as they are known within the [REDACTED] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [REDACTED] leveraged a **Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection**. The covert channel originates from users who use UCBrowser (mobile phone compact web browser). **The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in [REDACTED]** Initial investigation has determined that perhaps malware can be associated when the covert channel is established. [REDACTED] covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to XKEYSCOPE can search within this type of traffic based on their IMSI or IMEI to determine target presence

**TOP SECRET//SI**



# UCWeb – XKS Microplugin

			Datetime ▲	Highlights	Datetime End	Browser Version	Email Address	Handset Model	IMEI	IMSI	Global Title	Platform	Active User/I	Casenotation
1	<input type="checkbox"/>	<input type="checkbox"/>	1	2012-05-13 02:29:20		2012-05-13 02:29:23	8.0.3.107	@123movies	nokiae90-1		9379900100		java	E9DHL00000M0000
2	<input type="checkbox"/>	<input type="checkbox"/>	3	2012-05-13 06:00:59		2012-05-13 06:01:00	8.0.3.107	@123movies	nokiae90-1		9379900100		java	E9DHL00000M0000
3	<input type="checkbox"/>	<input type="checkbox"/>	4	2012-05-13 19:39:11		2012-05-13 19:39:11	7.9.3.103		HTC A510e				android	E9BDE00000M0000
4	<input type="checkbox"/>	<input type="checkbox"/>	2	2012-05-14 12:29:53		2012-05-14 12:29:53	8.0.4.121	@djgol	NokiaE72-1				sis	E9DHL00000M0000
5	<input type="checkbox"/>	<input type="checkbox"/>	5	2012-05-14 17:46:46		2012-05-14 17:46:46	8.0.4.121	@mobimasti	NokiaX6-00				sis	H5H125221450000
6	<input type="checkbox"/>	<input type="checkbox"/>	6	2012-05-15 18:28:19		2012-05-15 18:28:19	8.0.4.121	@mobimasti	NokiaX6-00		93781090013		sis	H5H125221450000
7	<input type="checkbox"/>	<input type="checkbox"/>	Z	2012-05-15 20:02:56		2012-05-15 20:02:56	8.0.4.121	@mobimasti	NokiaX6-00		93781090013		sis	H5H12522145000

TOP SECRET//SI



# Vision of Success

- \* Shared convergence database with numerous different sources, methods & tradecraft feeding into it
- \* Ultimately correlating telephony and Internet TDIs with some degree of confidence



# Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team  
(NTAT)

