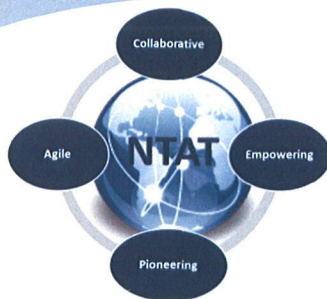


Synergising Network Analysis Tradecraft

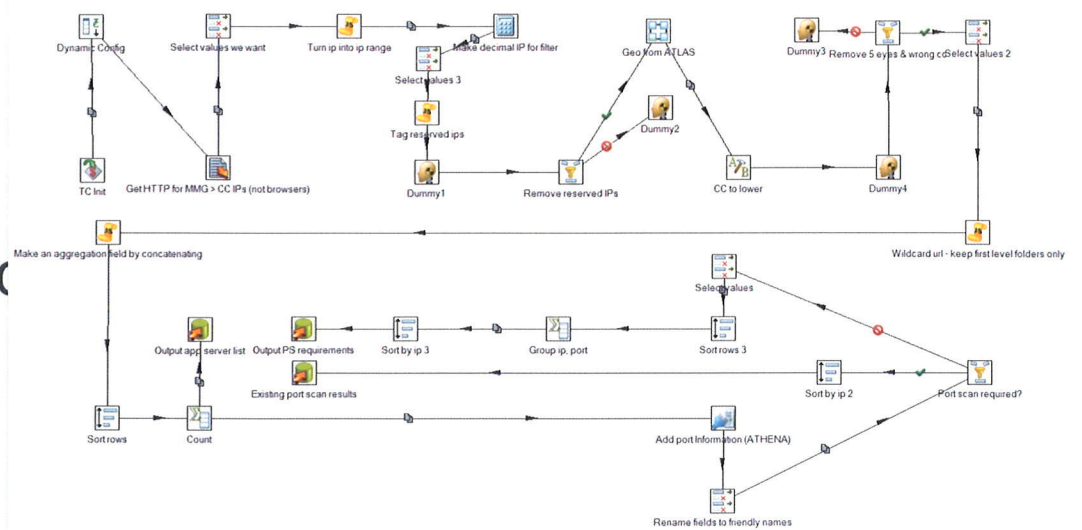
Network Tradecraft Advancement Team
(NTAT)



Overview

* What is the NTAT?

* 2011 – 2012 work and accomplishments



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

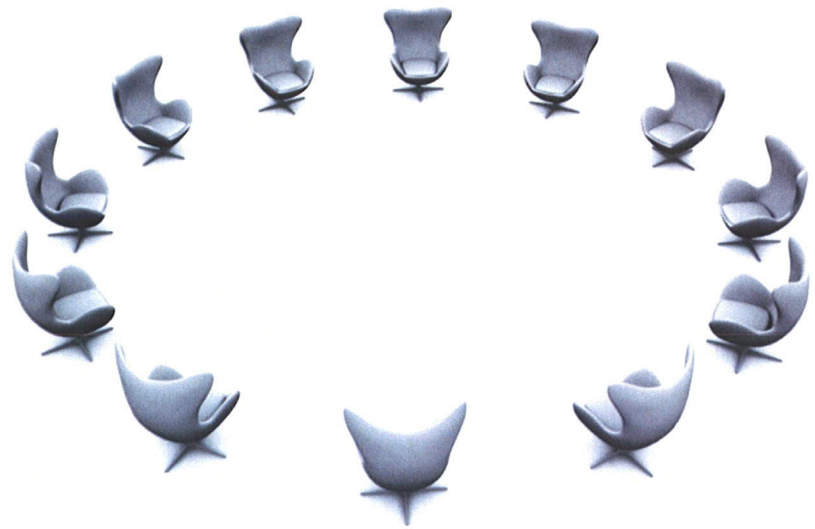


TOP SECRET//SI



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



DSD Workshop November 2011

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

<https://wiki.dsd/twiki/> [REDACTED]

TOP SECRET//SI



DSD Workshop Outcomes

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

- ∅ *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

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

DSD implementation of mobile gateway identification analytic based on FRETING YETI

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

CRAFTY SHACK trial

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

TOP SECRET//SI



XKS Microplugin: Samsung Protocol

State	ID	CSC	Device_Model	HTTP_User_Agent	IMEI	Latest_Mcc	Mcc	Message_Id	Message_Type	Mnc	Network_Ty	Odc_Versio	aded_	Postloaded_	Preloaded_	Preloaded_apps	Version	Active User#	Casenotation
1	353	1KSA	GT-N7000	SAMSUNG-Android		412	2306-8	checkAppUpgrade Request	50	0	2.6.084				com.sec.android.app.samsungapp@2.1.0a	1.0a		ESDHL00000M0000	
2	558	1AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0	1.0		ESDHL00000M0000	
3	548	1AUT	GT-P7500	SAMSUNG-Android		250	2306-1	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0	1.0		ESDHL00000M0000	
4	549	1AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0	1.0		ESDHL00000M0000	
5	1269	1AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0	1.0		ESDHL00000M0000	
6	1281	1AUT	GT-P7500	SAMSUNG-Android		250	2306-3	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0	1.0		ESDHL00000M0000	
7	1282	1AUT	GT-P7500	SAMSUNG-Android		250	2306-4	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
8	1274	1AUT	GT-P7500	SAMSUNG-Android		250	2306-5	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
9	1	1AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
10	67	1AUT	GT-P7500	SAMSUNG-Android		250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
11	433	1SKZ	GT-I9100	SAMSUNG-Android		412	2306-0	checkAppUpgrade Request	20	0	2.6.148				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
12	483	1XSG	GT-I9100	SAMSUNG-Android		412	2350-0	getPushNotificationMessage Re	20	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
13	1074	1XSG	GT-I9100	SAMSUNG-Android		412	2350-0	getPushNotificationMessage Re	20	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
14	786	1XSG	GT-I9100	SAMSUNG-Android		412	2309-0	getDownloadList Request	20	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
15	1119	1XSG	GT-I9100	SAMSUNG-Android		412	2308-0	getKillList Request	20	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
16	664	1XSG	GT-I9100	SAMSUNG-Android		412	2301-0	getUpgradeNKillCount Request	20	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
17	360	1XSG	GT-I9100	SAMSUNG-Android		412	2301-0	getUpgradeNKillCount Request	50	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
18	282	1XSG	GT-I9100	SAMSUNG-Android		412	2309-0	getDownloadList Request	50	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
19	490	1XEU	GT-I9100	SAMSUNG-Android		412	2302-2	upgradeListEx Request	20	0	2.6.194				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
20	522	1XEU	GT-I9100	SAMSUNG-Android		412	2160-6	purchaseDetailEx Request	20	0	2.6.194				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
21	951	1XSG	GT-I9100	SAMSUNG-Android		412	2306-2	checkAppUpgrade Request	20	0	2.6.048				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
22	954	1THR	GT-B5512	SAMSUNG-Android		412	2306-5	checkAppUpgrade Request	40	0	2.6.122				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
23	955	1XSG	GT-I9100	SAMSUNG-Android		412	2302-2	upgradeListEx Request	20	0	2.6.194				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
24	958	1XSG	GT-I9100	SAMSUNG-Android		412	2306-2	checkAppUpgrade Request	20	0	2.6.048				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
25	1259	1XSG	GT-I9100	SAMSUNG-Android		412	2306-2	checkAppUpgrade Request	20	0	2.6.048				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
26	1344	1XSG	GT-I9100	SAMSUNG-Android		412	2306-2	checkAppUpgrade Request	20	0	2.6.048				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
27	1500	1XSG	GT-I9100	SAMSUNG-Android		412	2306-2	checkAppUpgrade Request	20	0	2.6.048				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
28	54	TOP SECRET//SI//	2012-05-11 06:43:27			412	2300-0	countrySearchEx Request	20	0					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
29	417	TOP SECRET//SI//	2012-05-13 02:32:35			412	2200-1	countrySearch Request	111	111					com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	
30	488	TOP SECRET//SI//	2012-05-11 09:32:39			412	5060-1	termInformation Request	20	0	2.6.048				com.sec.android.app.samsungapp 1.0a	1.0a		ESDHL00000M0000	

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



Winter Nirvana



The Reality!



CSE Workshop Outcomes

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

Ø *17 XKS fingerprints deployed*

Documentation of analytics in CRAFTY SHACK

Ø *These analytics are now being implemented across the 5 Eyes*

Proving the tradecraft actually works!

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

TOP SECRET//SI



Op IRRITANT HORN



TOP SECRET//SI



Op IRRITANT HORN

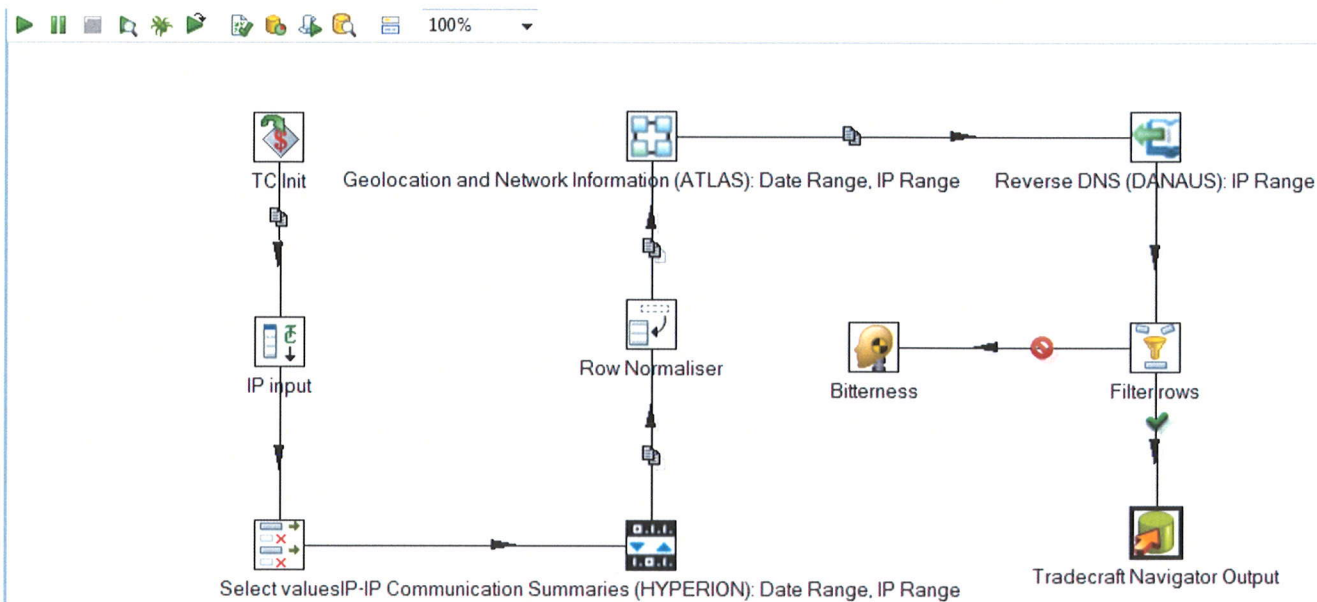
Does the tradecraft work?

- * 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

TOP SECRET//SI



Finding mobile application & vendor update servers



TOP SECRET//SI



Finding mobile application & vendor update servers

100%



TOP SECRET//SI





Change view [icon] [redacted]@cse-cst.gc.ca

Search this wiki

Go Search

Home Browse Search Create Help MediaWiki

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 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]
 Agency: NSA
 Email Address: [redacted]

Difficulty: ★★
 Acceptance state: Limited

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.

- Take IP ranges or individual addresses identified as being related to mobile network communications.
- Obtain geolocation information and network ownership information for each IP address. This should include: Network Owner name, Carrier name, ASN, Continent, Country, Region, City, Lat, Long, and any other related details that your system can obtain.
- 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.
- Sort the results and dedup them. This step depends on your collection sources.
- 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
- 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
- Sort and dedup again based on Server IP information. TCP Direction info is no longer needed.
- 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.
- Remove any servers that are not useful. This may include 5-Eyes servers.
- Output
 - List of Servers
 - List of related User Agents
 - List of related hostnames

Comments (2) | Show comments

Average article quality based on 1 rating(s)

Last updated: 24/2/2012 by [redacted]

Category: Tradecraft

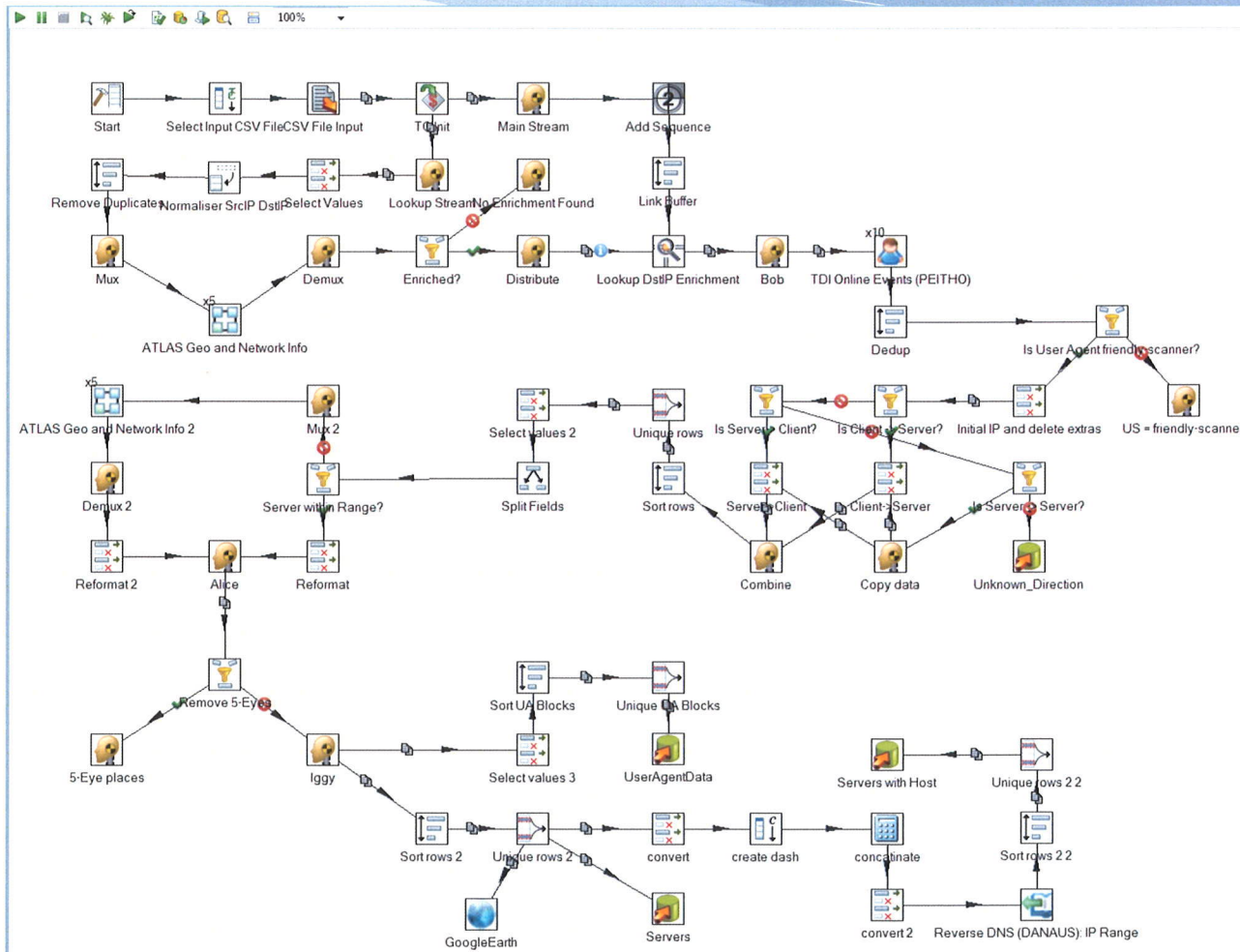
CRAFTY SHACK - "It's not tradecraft until it's documented" - CSEC

[edit]

TOP SECRET//SI



Identifying servers communicating with an MNO

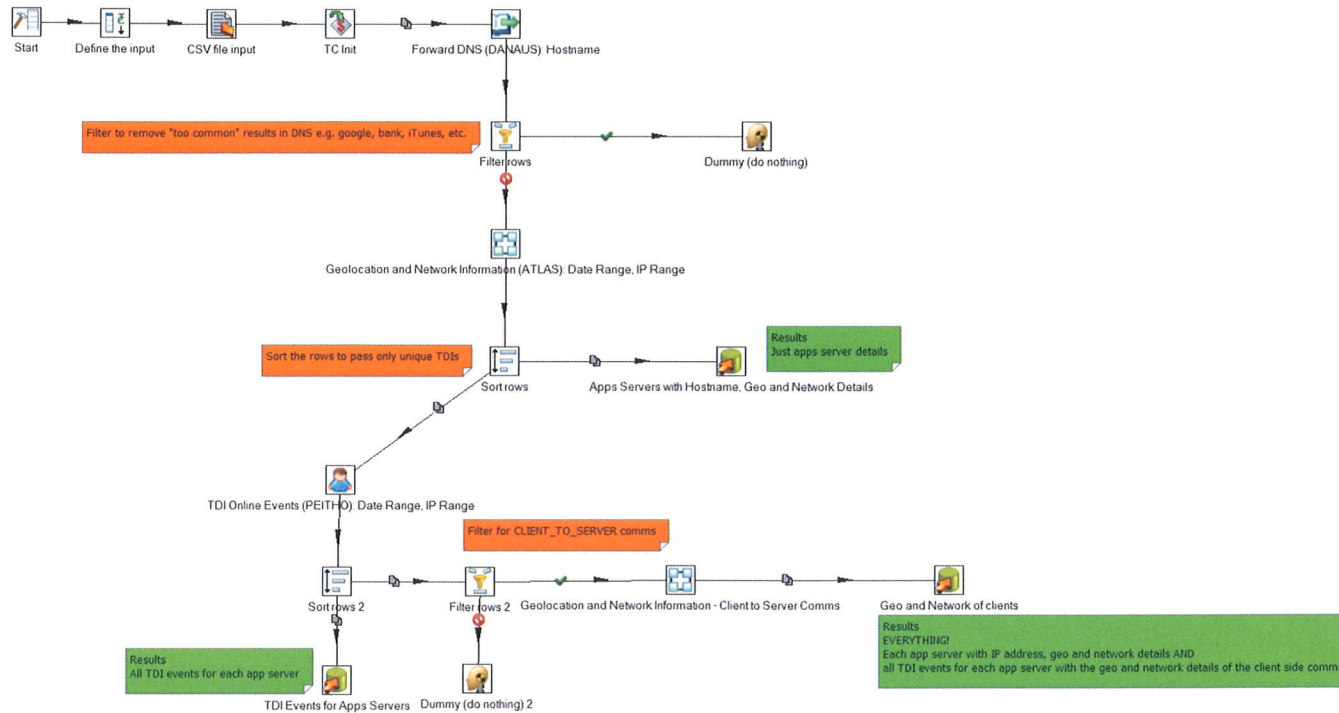


TOP SECRET//SI



Profiling mobile application servers

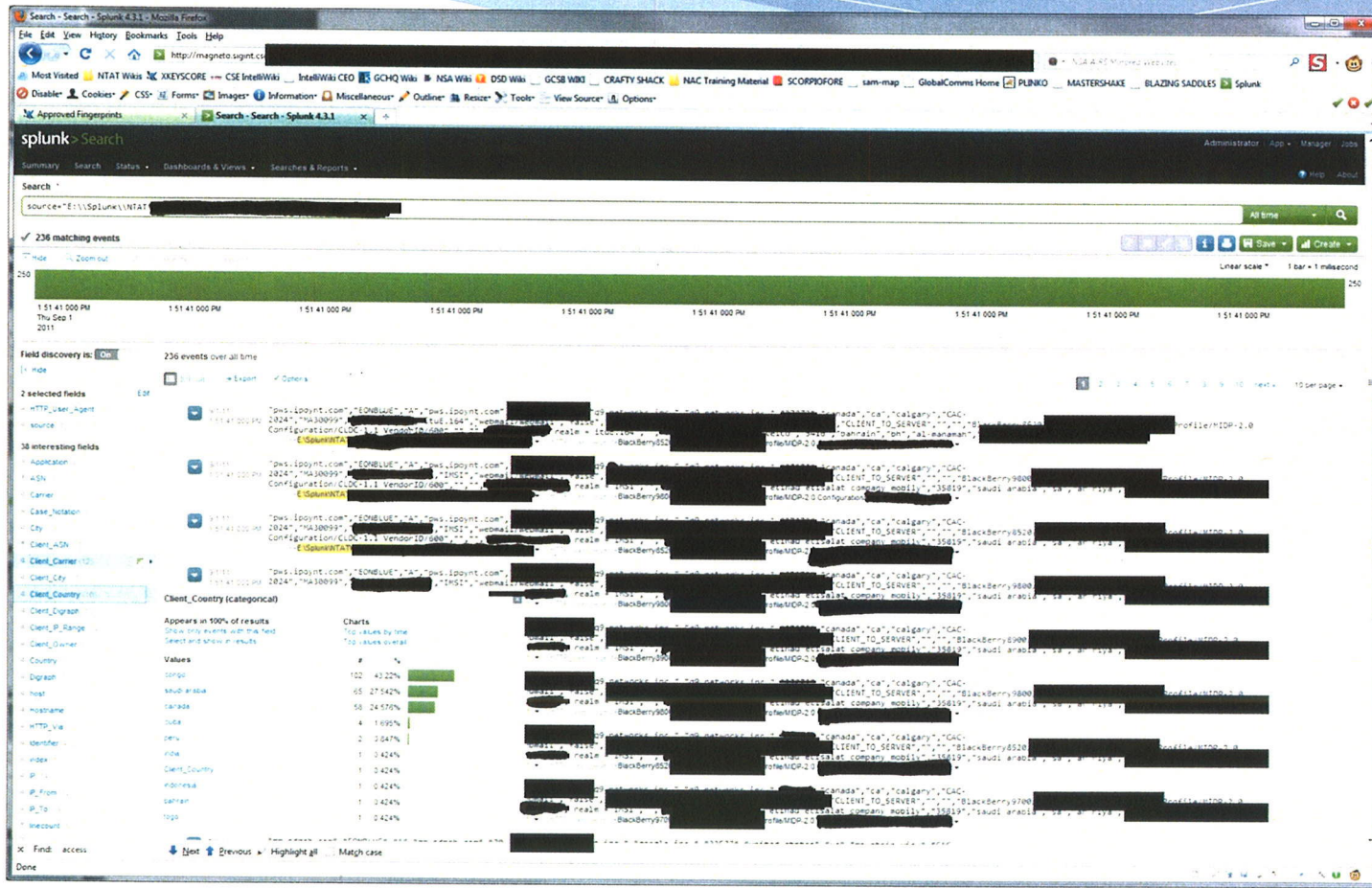
This tradecraft will accept a CSV file of known apps server hostnames. It will then perform reverse DNS queries to obtain the IP addresses of the apps servers. With the IP addresses, geolocation and network provider queries will be performed on all app server IP addresses. The IP addresses are then used 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



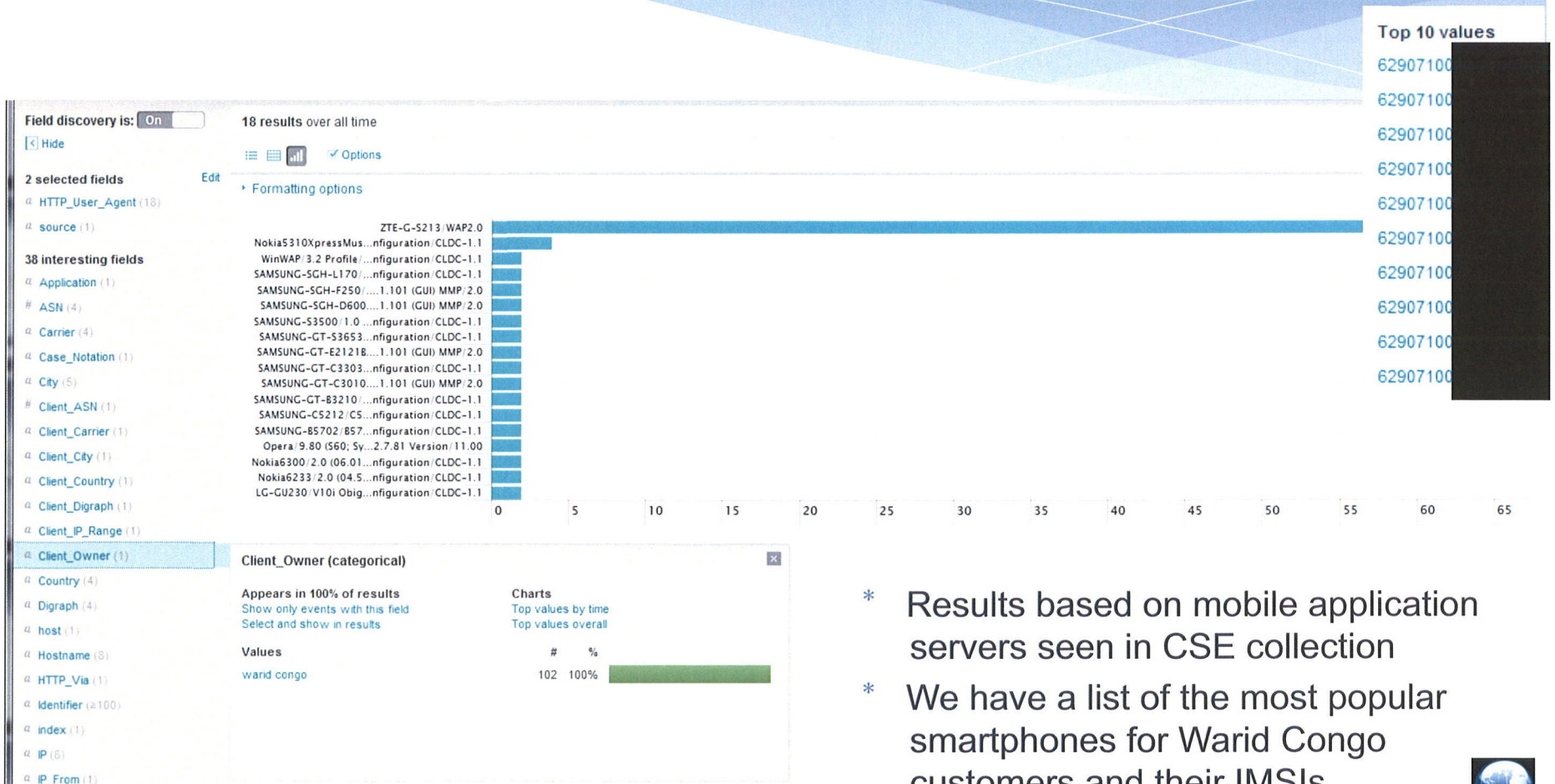
Profiling mobile application servers



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 X-KEYSCOPE can search within this type of traffic based on their IMSI or IMEI to determine target presence*

TOP SECRET//SI



UCWeb – XKS Microplugin

UCWeb														
Help Actions Reports View Map View														
	State	ID	Datetime	Highlights	Datetime End	Browser Version	Email Address	Handset Model	IMEI	IMSI	Global Title	Platform	Active User/	Casenotation
1		1	2012-05-13 02:29:20		2012-05-13 02:29:23	8.0.3.107	@123movies	nokiae90-1			9379900100	java		E9DHL00000M0000
2		3	2012-05-13 06:00:59		2012-05-13 06:01:00	8.0.3.107	@123movies	nokiae90-1			9379900100	java		E9DHL00000M0000
3		4	2012-05-13 19:39:11		2012-05-13 19:39:11	7.9.3.103		HTC A510e				android		E9BDE00000M0000
4		2	2012-05-14 12:29:53		2012-05-14 12:29:53	8.0.4.121	@djgol	NokiaE72-1				sis		E9DHL00000M0000
5		5	2012-05-14 17:46:46		2012-05-14 17:46:46	8.0.4.121	@mobimasti	NokiaX6-00				sis		H5H125221450000
6		6	2012-05-15 18:28:19		2012-05-15 18:28:19	8.0.4.121	@mobimasti	NokiaX6-00			93781090013	sis		H5H125221450000
7		7	2012-05-15 20:02:58		2012-05-15 20:02:58	8.0.4.121	@mobimasti	NokiaX6-00			93781090013	sis		H5H125221450000

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)

