

Identifier Lead Triage with ECHOBASE



[REDACTED]
NSA - S2I51
NSA - T1442

JUN 2012



The Problem

SIGINT is very good at 2 things:

1. Establishing lists of potential leads (50-10k+)
2. Manual analysis to vet individual targets

A funnel diagram representing a process flow. The top section is shaded grey and contains the text "Potential leads 50-10k+". The middle section is also grey and contains four question marks ("????"). The bottom section is grey and contains the text "Manual analysis". The funnel tapers from top to bottom, indicating a reduction in the number of leads being analyzed.

Potential leads
50-10k+

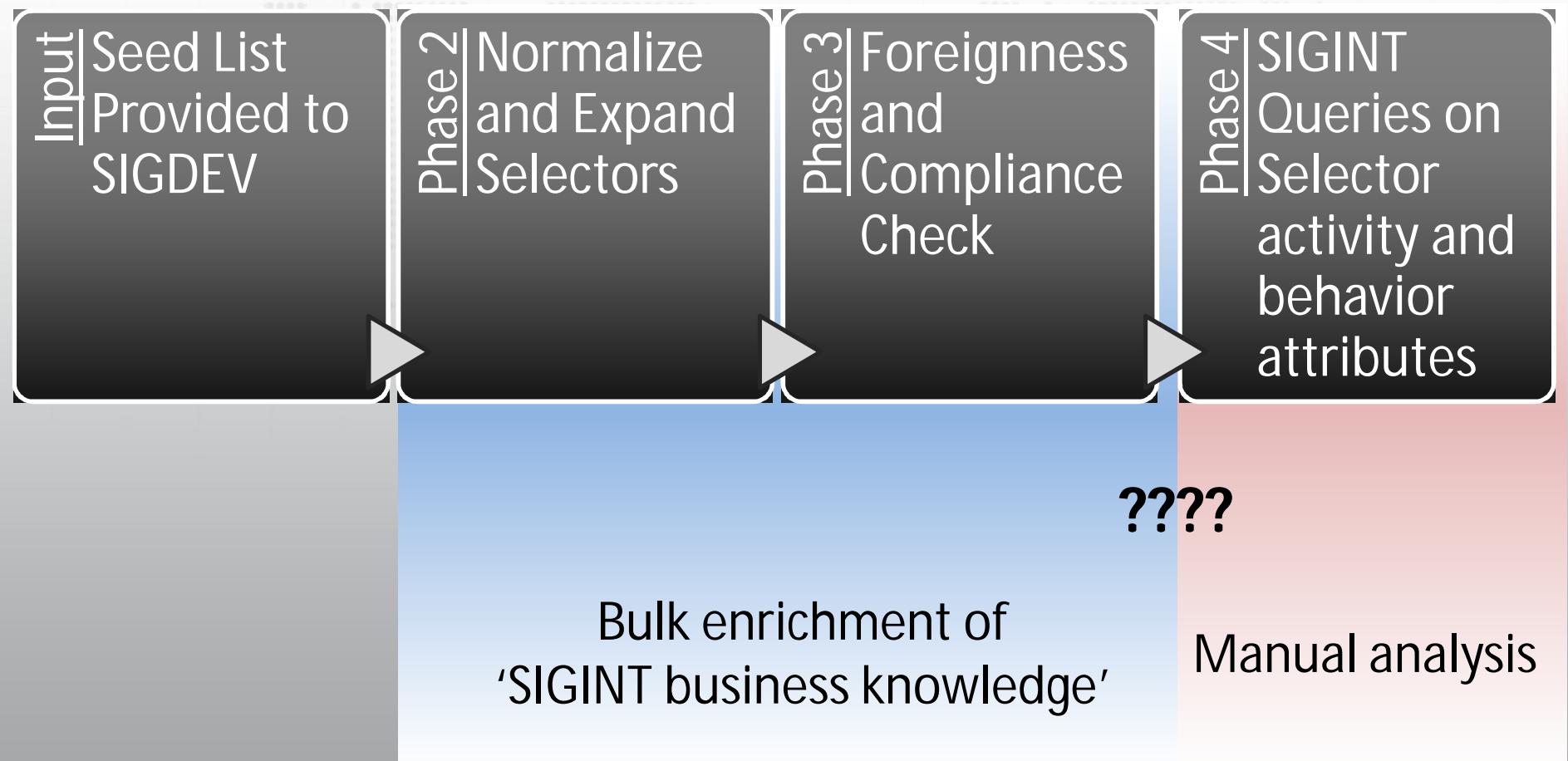
????

Manual
analysis



Tradecraft

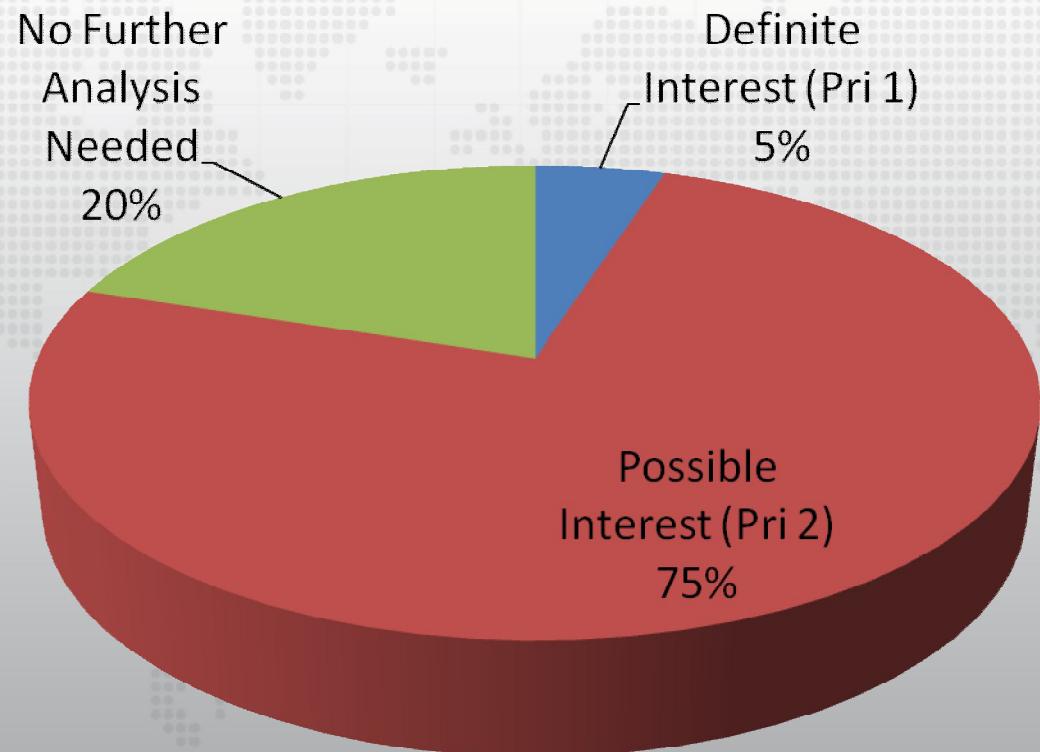
A common model for identifier lead lists, today:





Triage Today

After initial enrichment checks, the analyst is often left with too many identifiers of “possible interest”

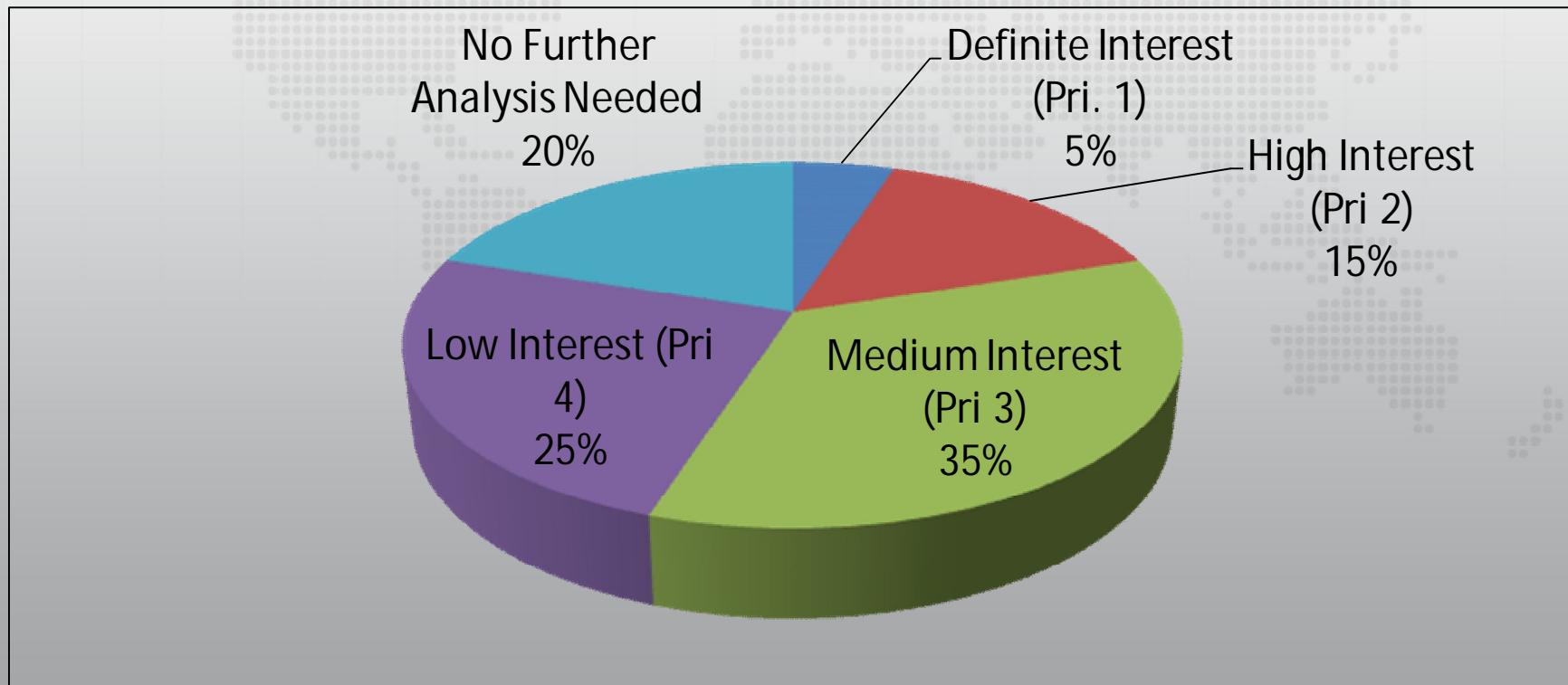


Percentages are conceptual



Bulk Lead Triage via Behavior Analytics

- Hundreds or thousands of selectors to go through high level vetting very quickly
- Better triage prioritization allows for highly adjustable thresholds to be set for follow -on analysis
- Compliance can be inserted at both the “batch result” and “query” level
- Potentially utilize multiple clouds & cross-enterprise analytics





Identifier 'SIGINT Business' Enrichment

Bulk gathering, via Identifier Scoreboard (phase 2/phase 3)

- Targeting
- Authorities
- Reporting
- Targets
- Knowledge
- Foreignness
- Compliance

*...not a raw
SIGINT query*

Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY

IDENTIFIER SCOREBOARD

Airport Threat

Add identifiers

Context	Realm
12147	[REDACTED]
[REDACTED]	yahoo
[REDACTED]	skypeUser

Import identifiers

Targeting tag: flag

Targeting category: [REDACTED]

Targeting zipcode: [REDACTED]

Query/criteria list: [REDACTED]
Priority Email: [REDACTED]
Choose...

Target: [REDACTED]
Choose...

Retrieve up-to-date FOREMAN data

Include correlations

Clear Save Search

SIGINT ANALYTICS

Identifier view Target view

Create target Customize Send to...

Normalized identifier	Comms	PSC	Tip	TAO	CNE	POCs	Targeting	Foreignness	Knowledge	Actions
[REDACTED]						1	n/a	Unkown		[REDACTED]
[REDACTED]						1	n/a	Unkown		[REDACTED]
[REDACTED]							(S2I12)	n/a	Unkown	[REDACTED]
[REDACTED]						4	n/a	Unkown	3	[REDACTED]

Last updated: 2012-Mar-01 09:58:46 Z

Displaying 1-100 of 154 page 1 of 2

Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY



'Yes/No' Identifier Behavior

Bulk triage, via SIGINT Analytics Mode (start of phase 4)

Core set of
'yes/no'
behavioral
questions
about a set of
identifier leads

*...against raw
SIGINT!*

Dynamic Page - Highest Possible Classification Is TOP SECRET//SI//REL TO USA, FVEY

SIGINT

Airport Threat

Identifier view Target view

Has this identifier been in direct communications with a targeted identifier?

Identifiers supported: DNI and DNR
Legal authorities: EO12333_S, EO12333_X, FAA_702_CP, FAA_702_CT, FAA_02_FG, FAA 704/705B
Results updated: Daily

Normalized identifier	Positive Results	Direct Comms with Target?	Targeted Contact?	In Captured Media?	Actions
[REDACTED]	2	*	n/a	n/a	[REDACTED]
[REDACTED]	n/a				[REDACTED]
[REDACTED] <msnpassport>	4		Targets: [REDACTED] <yahoo> TP [REDACTED] [REDACTED] <facebookname> TP [REDACTED]		[REDACTED] First heard: 03 Dec 2011 Last heard: 29 Feb 2012
[REDACTED] <yahoo>	3	*			[REDACTED]
[REDACTED] <emailAddr>	n/a				[REDACTED]
[REDACTED] <msnpassport>	4	*	*		[REDACTED]
[REDACTED] <facebookname>	2		*		[REDACTED]
[REDACTED] <skypeUser>	0				[REDACTED]
[REDACTED] <yahoo>	0				[REDACTED]
[REDACTED] <yahoo>	2	*			[REDACTED]
[REDACTED] <emailAddr>	2		*		[REDACTED]
[REDACTED] <msnpassport>	0				[REDACTED]
[REDACTED] <google>	0				[REDACTED]
[REDACTED]	0		n/a	n/a	[REDACTED]
[REDACTED]	2	*			[REDACTED]
[REDACTED]	4	*	*	*	[REDACTED]
[REDACTED]	2	*	n/a	n/a	[REDACTED]

Last ran on: 2012-Mar-01 09:58:46 Z

Displaying 1-100 of 148 | page 1 of 2

(U//FOUO) Page Publisher: Identifier Scoreboard, T1422 | Content [REDACTED] T14 | Last Reviewed: 15-Dec-2010 | Last Modified: 23-Feb-2012
(U//FOUO) Derived From: NSA/CSSM 1-52 | Declassify On: 20320108 | Dated: 08 January 2007

Dynamic Page - Highest Possible Classification is TOP SECRET//SI//REL TO USA, FVEY



SIGINT Analytics Mode

Triage by aggregate behaviors

The screenshot shows a table with columns for 'Normalized identifier', 'Positive Results', 'Direct Comms with Target?', 'Targeted Contact?', 'In Captured Media?', and several other columns that are mostly redacted. One row is expanded to show more details:

Normalized identifier	Positive Results	Direct Comms with Target?	Targeted Contact?	In Captured Media?
[REDACTED]	2	*	n/a	n/a	n/a	...
[REDACTED]	n/a					...
[REDACTED] <msnpassport>	4	Targets: [REDACTED] <yahoo> TP [REDACTED] [REDACTED] <facebookname> TP [REDACTED]				First heard: 03 Dec 2011 Last heard: 29 Feb 2012
[REDACTED] <yahoo>	3	*				
[REDACTED] <emailAddr>	n/a					
[REDACTED] <msnpassport>	4	*	*	*	*	
[REDACTED] <facebookname>	2		*	*		
[REDACTED] <skypeUser>	0					
[REDACTED] <yahoo>	0					
[REDACTED] <yahoo>	2	*				
[REDACTED] <emailAddr>	2		*			

One column per 'yes/no' question

Quickly zero in on worthy leads

SIGINT Analytics Mode – Detailed View



Dynamic Page - Highest Possible Classification Is **TOP SECRET//SI//REL TO USA, FVEY**

SIGINT ANALYTICS

Analytic Results: <msnpassport> ✓ 2012-Mar-01 09:58:46 Z

Had direct communications with a targeted identifier? [REDACTED] [View in Target Profiler](#)

Seen in captured media? (no results)

Seen in CNE? (no results)

Seen in France?

Seen on a targeted identifier's contact lists, or has a targeted contact? (no results)

▼ Had direct communications with a targeted identifier?

First heard: 2012-Mar-01 08:58:42 Z Last heard: 2012-Mar-05 07:55:40 Z

Date	Description	Source
2012-Mar-05 07:55:40 Z	[REDACTED] <msnpassport> cc'd email to [REDACTED]<yahoo>	UUID: [REDACTED] SIGAD/PDDG: DS-200A / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-04 09:58:46 Z	[REDACTED] <msnpassport> was bcc'd on email from <msnpassport>	UUID: [REDACTED] SIGAD/PDDG: DS-200A / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-02 10:56:43 Z	[REDACTED] <msnpassport> received email from <msnpassport>	UUID: [REDACTED] SIGAD/PDDG: DS-200B / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-01 08:58:42 Z	[REDACTED] <msnpassport> sent email to [REDACTED]<yahoo>	UUID: [REDACTED] SIGAD/PDDG: US-3171 / T8 Case notation: [REDACTED] Legal authority category: EO12333

[Back to top](#)

(U//FOUO) Page Publisher: Identifier Scoreboard, T1422 | Content [REDACTED] T14 | Last Reviewed: 15-Dec-2010 | Last Modified: 23-Feb-2012
 (U//FOUO) Derived From: NSA/CSSM 1-52 | Declassify On: 20320108 | Dated: 08 January 2007

Dynamic Page - Highest Possible Classification is **TOP SECRET//SI//REL TO USA, FVEY**

SIGINT Analytics Mode – Detailed View



▼ Had direct communications with a targeted identifier?

First heard: 2012-Mar-01 08:58:42 Z **Last heard:** 2012-Mar-05 07:55:40 Z

Date	Description	Source
2012-Mar-05 07:55:40 Z	[REDACTED] cc'd email to [REDACTED]	UUID: [REDACTED] SIGAD/PDDG: DS-200A / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-04 09:58:46 Z	[REDACTED] was bcc'd on email from [REDACTED]	UUID: [REDACTED] SIGAD/PDDG: DS-200A / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-02 10:56:43 Z	[REDACTED] received email from [REDACTED]	UUID: [REDACTED] SIGAD/PDDG: DS-200B / C4 Case notation: [REDACTED] Legal authority category: EO12333
2012-Mar-01 08:58:42 Z	[REDACTED] sent email to [REDACTED]	UUID: [REDACTED] SIGAD/PDDG: US-3171 / T8 Case notation: [REDACTED] Legal authority category: EO12333

[Back to top](#)

Go view target knowledge

Go view content

Add new knowledge

External links to guide next steps in analysis



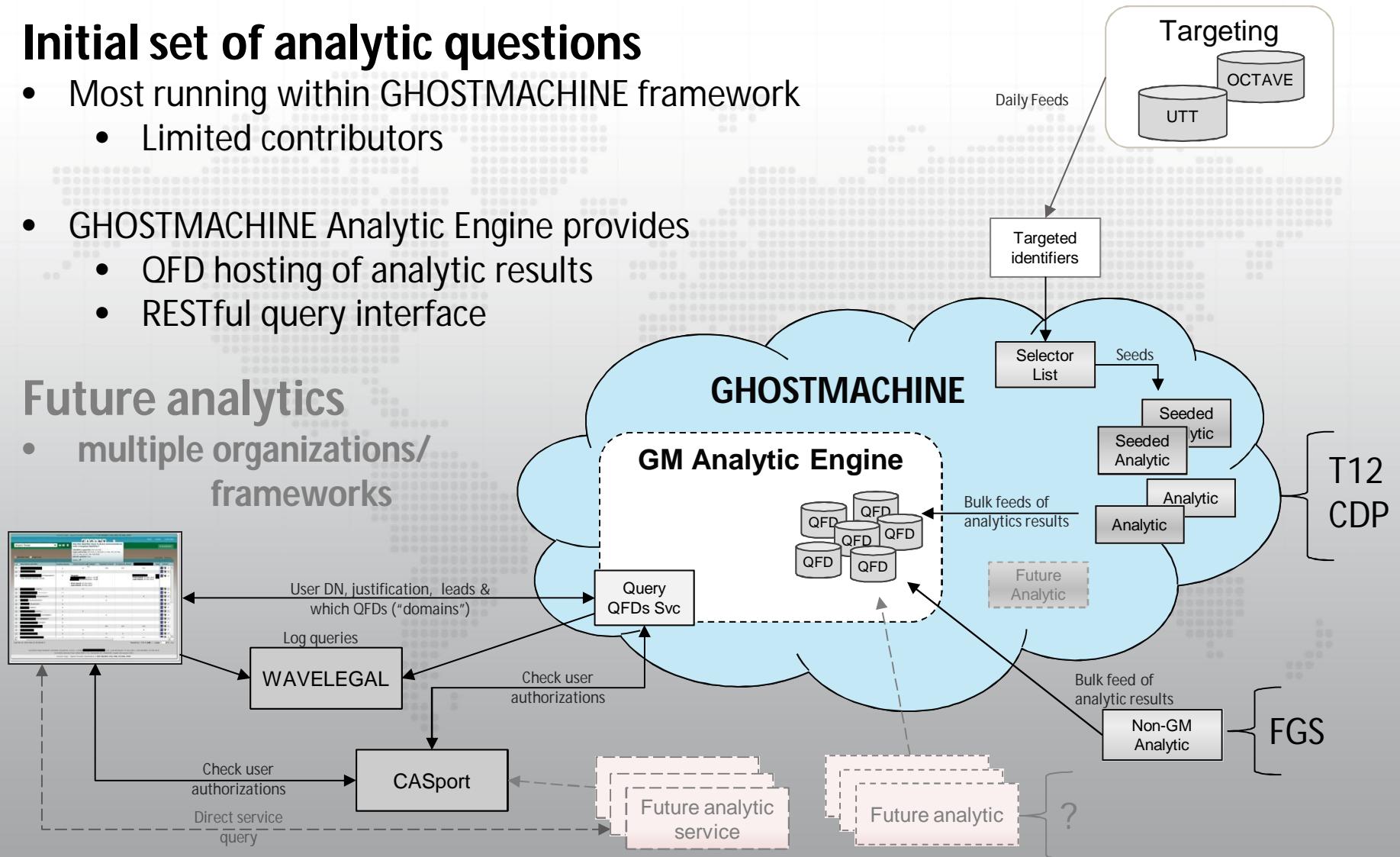
ECHOBASE Analytics Architecture

Initial set of analytic questions

- Most running within GHOSTMACHINE framework
 - Limited contributors
- GHOSTMACHINE Analytic Engine provides
 - QFD hosting of analytic results
 - RESTful query interface

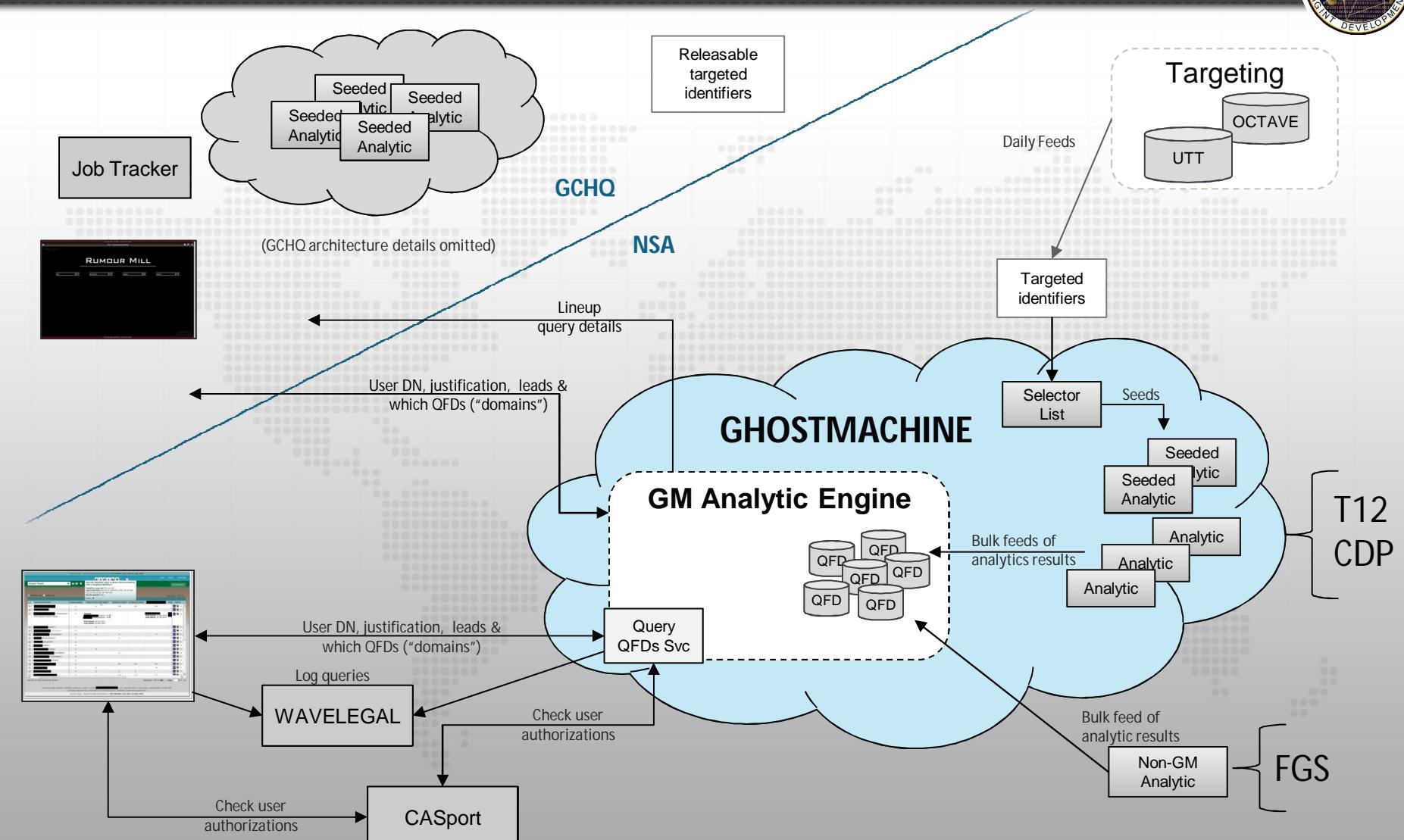
Future analytics

- multiple organizations/
frameworks





2012 Olympics Sharing



2012 Olympics Support



- NSA SID Leads Evaluation Cell
 - Triage of Olympics-based leads through the event
 - Leverage both NSA and GCHQ-produced analytics
- Greater SID-wide usage following the Olympic period



Contact/Information

- Briefers:
 - [REDACTED]
 - [REDACTED]
- ECHOBASE Alias:
 - [REDACTED]
- NSA WikInfo page:
 - [REDACTED]