Identifier Lead Triage with ECHOBASE

[redacted]

NSA - S2I51
NSA - T1442

JUN 2012

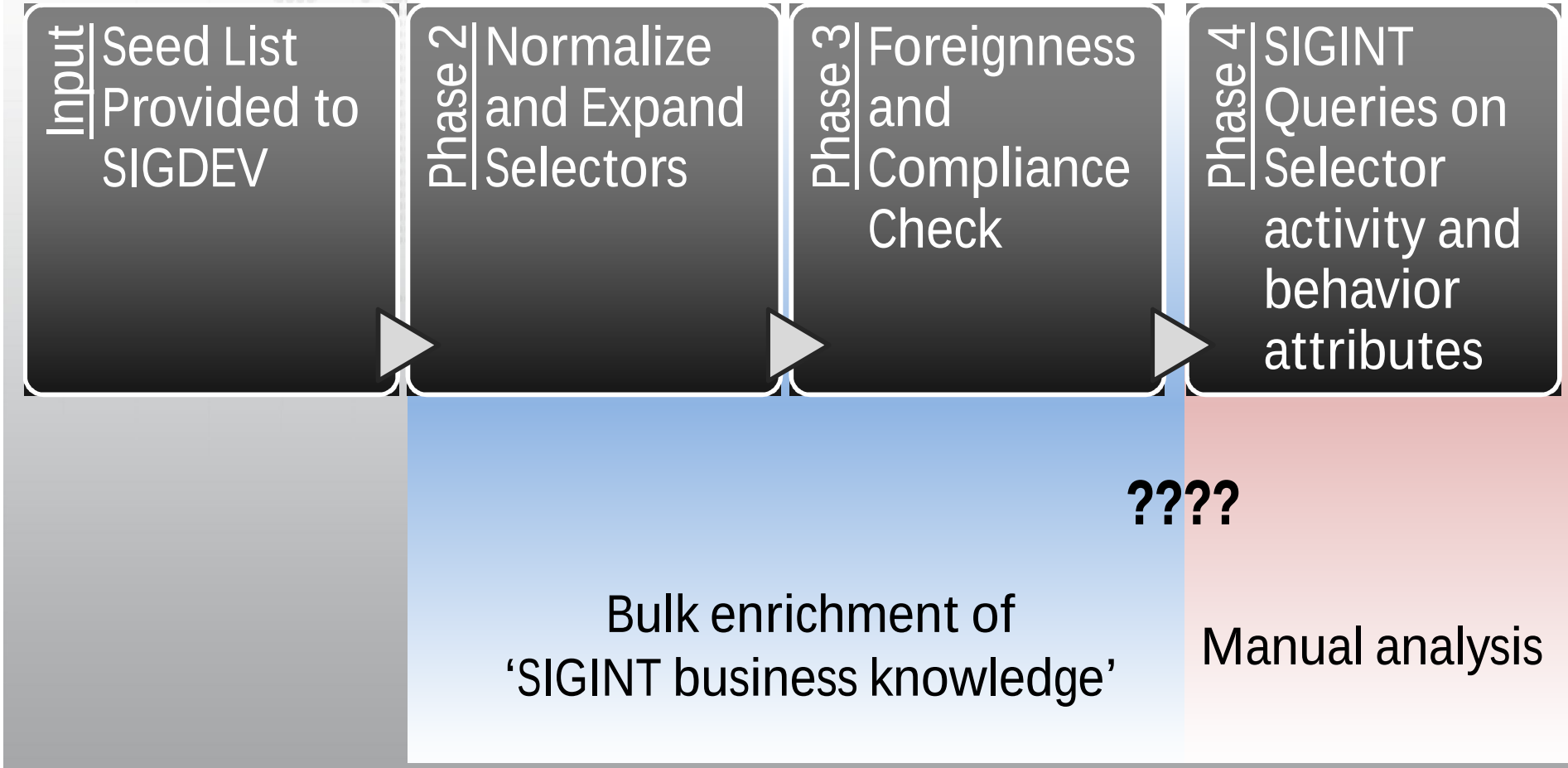
The Problem

SIGINT is very good at 2 things:

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

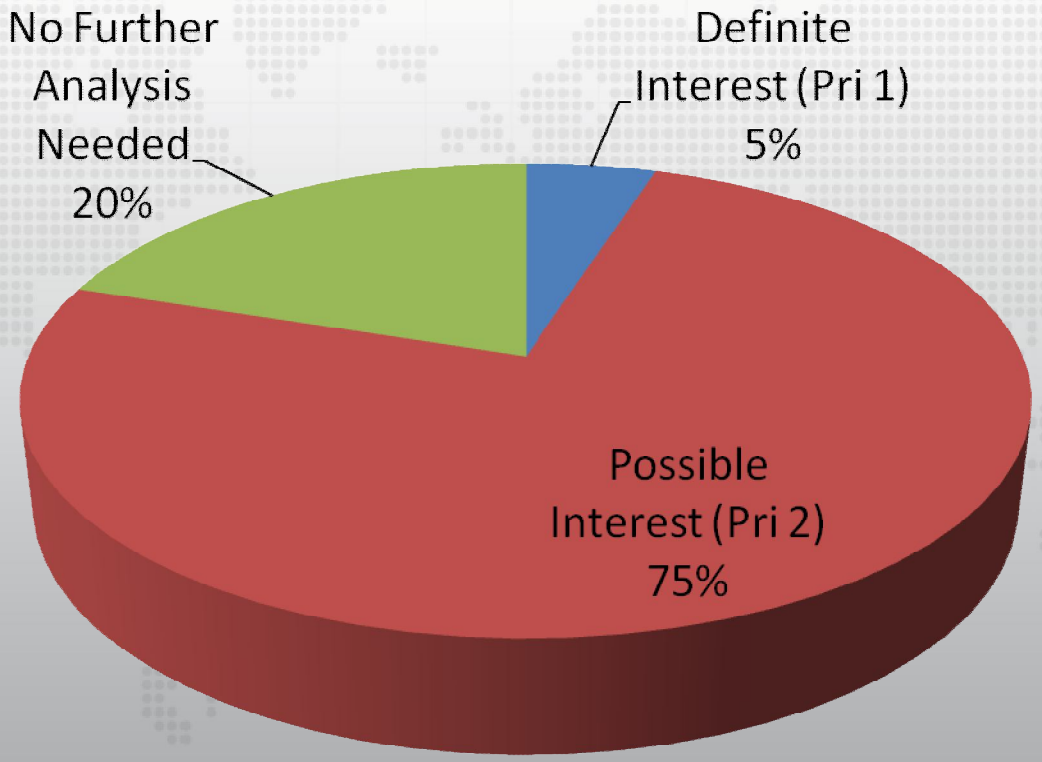
Tradecraft

A common model for identifier lead lists, today:



Triage Today

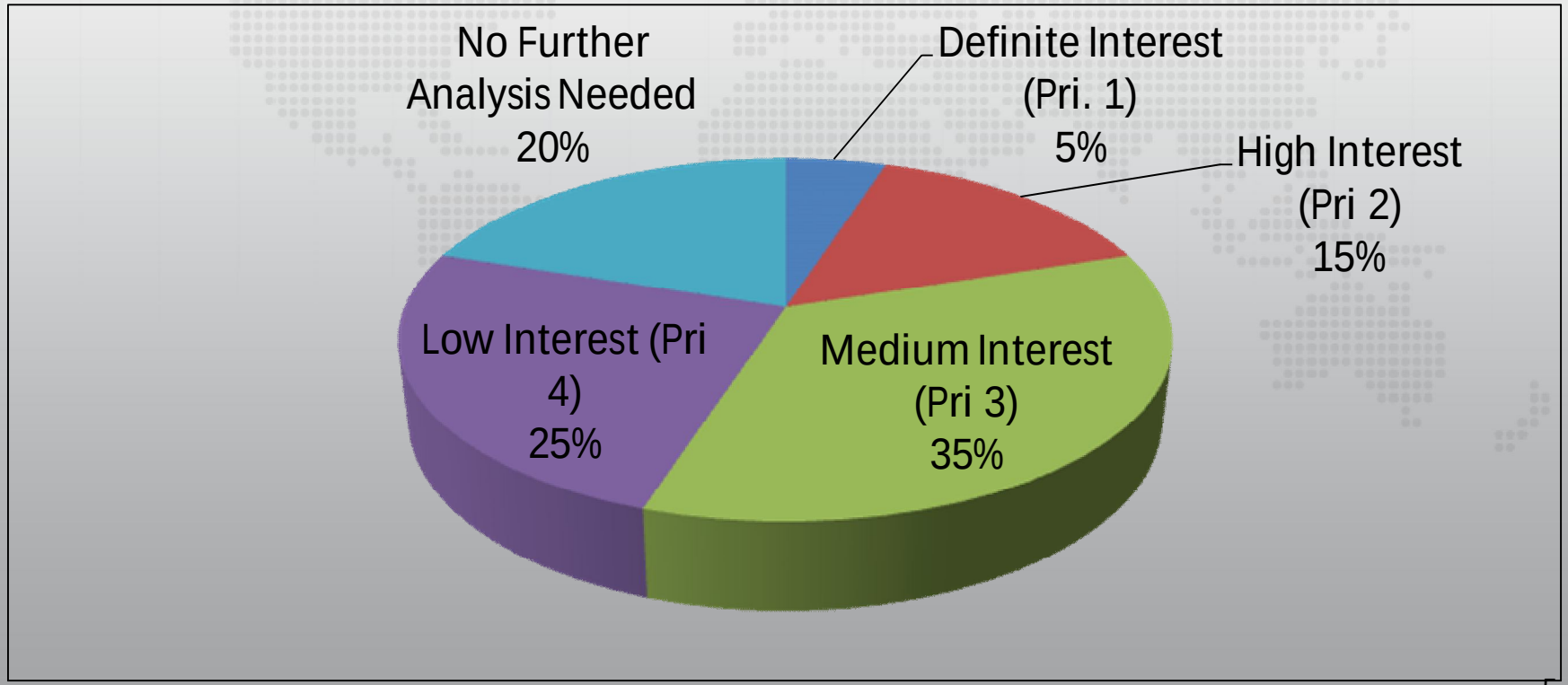
After initial enrichment checks, the analyst is often left with too many identifiers of "possible interest"



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

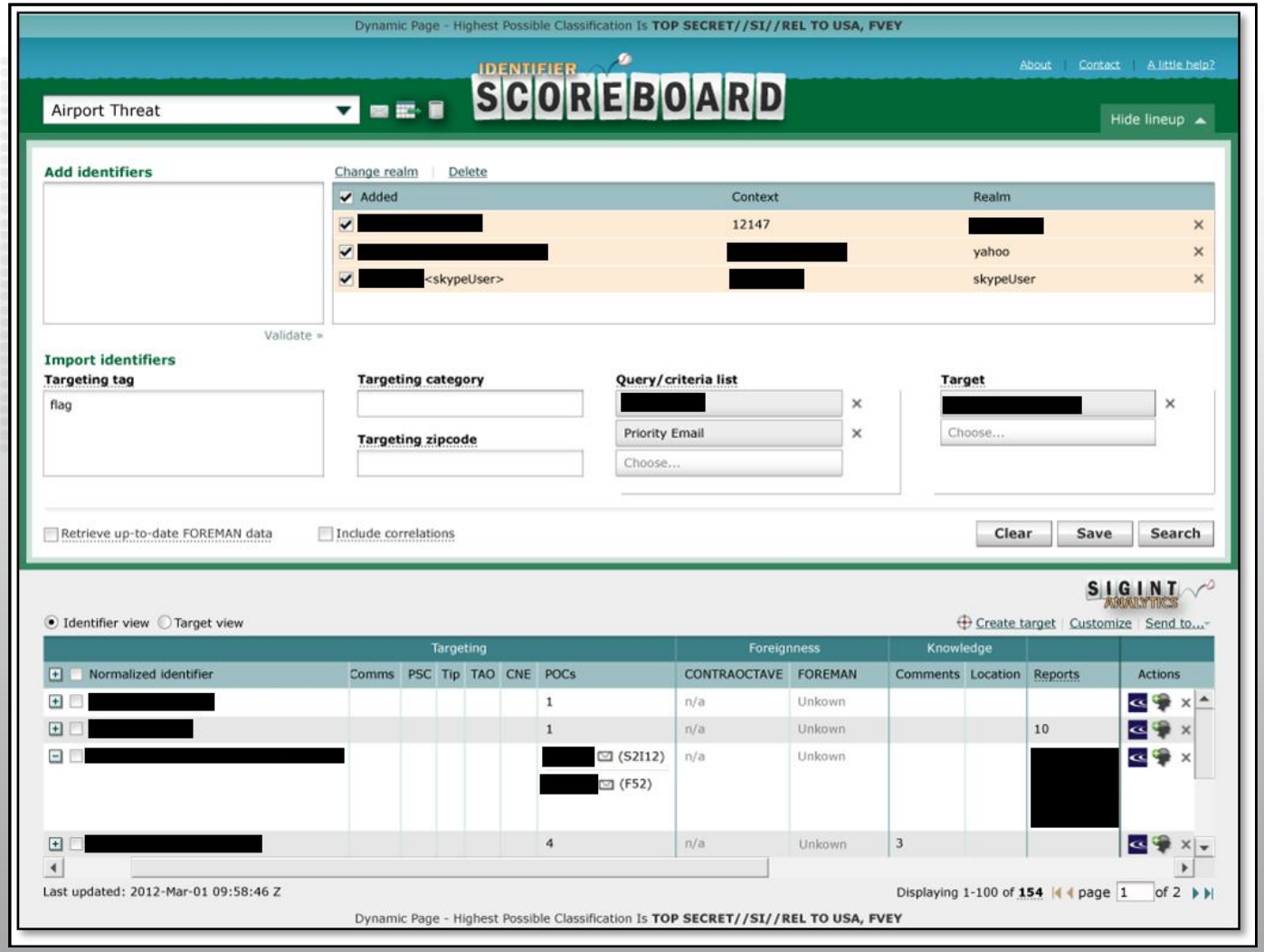


Identifier 'SIGINT Business' Enrichment

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

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

...not a raw SIGINT query

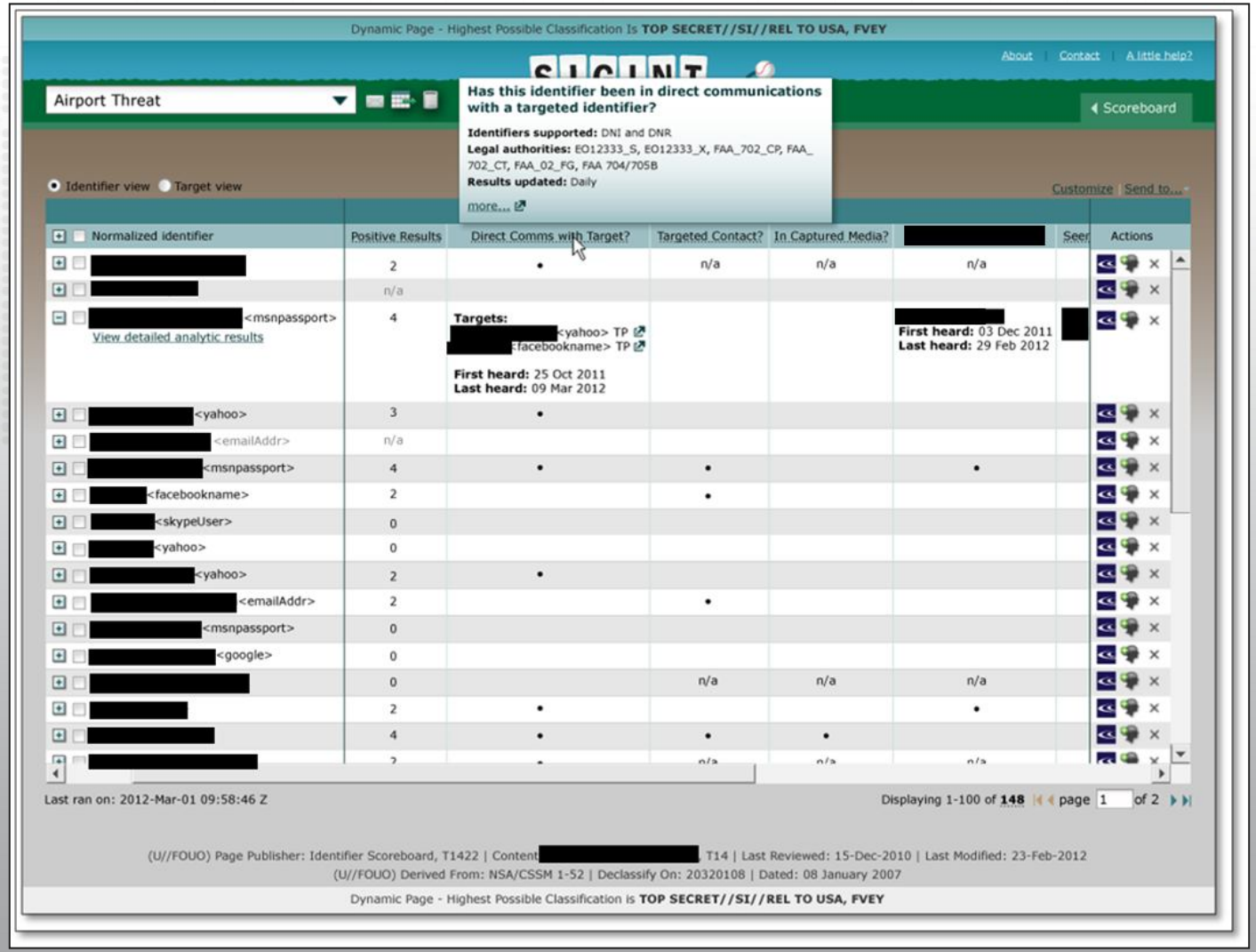


'Yes/No' Identifier Behavior

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

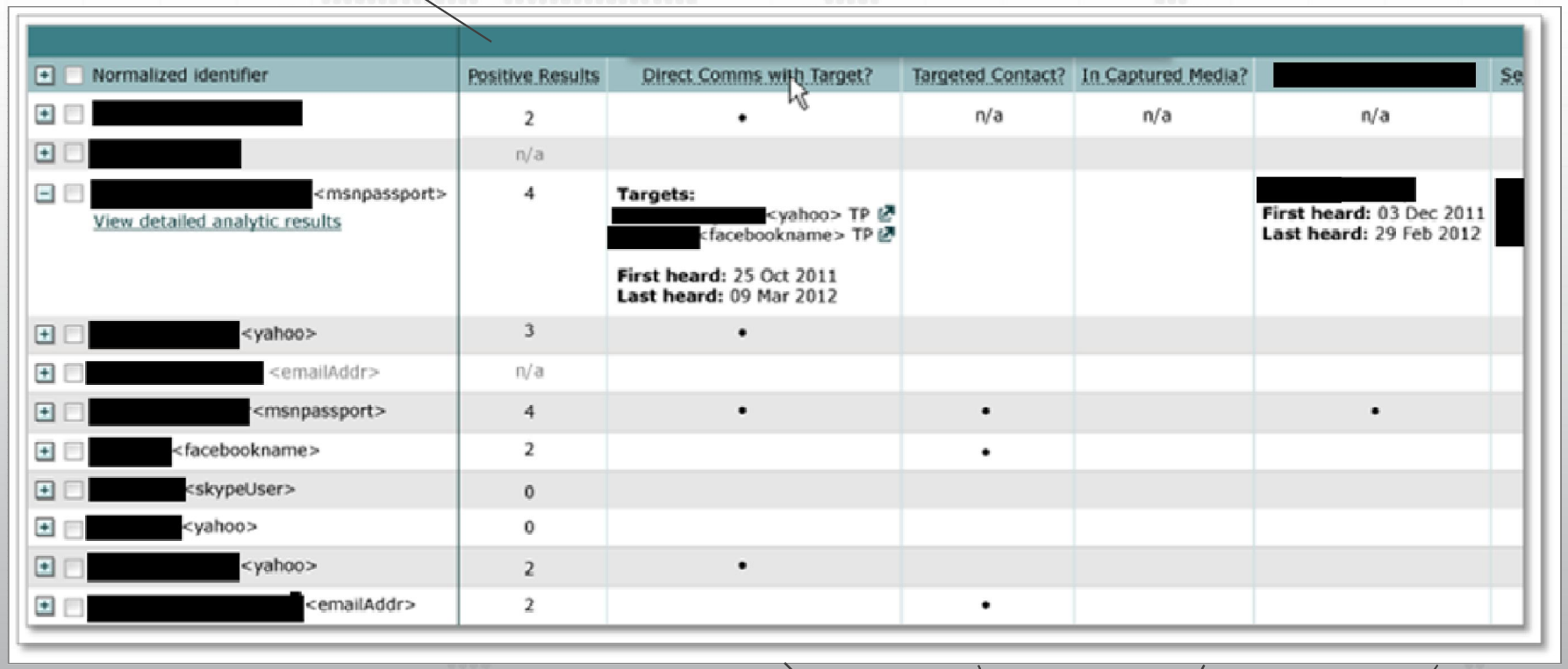
Core set of 'yes/no' behavioral questions about a set of identifier leads

...against raw SIGINT!



SIGINT Analytics Mode

Triage by aggregate behaviors

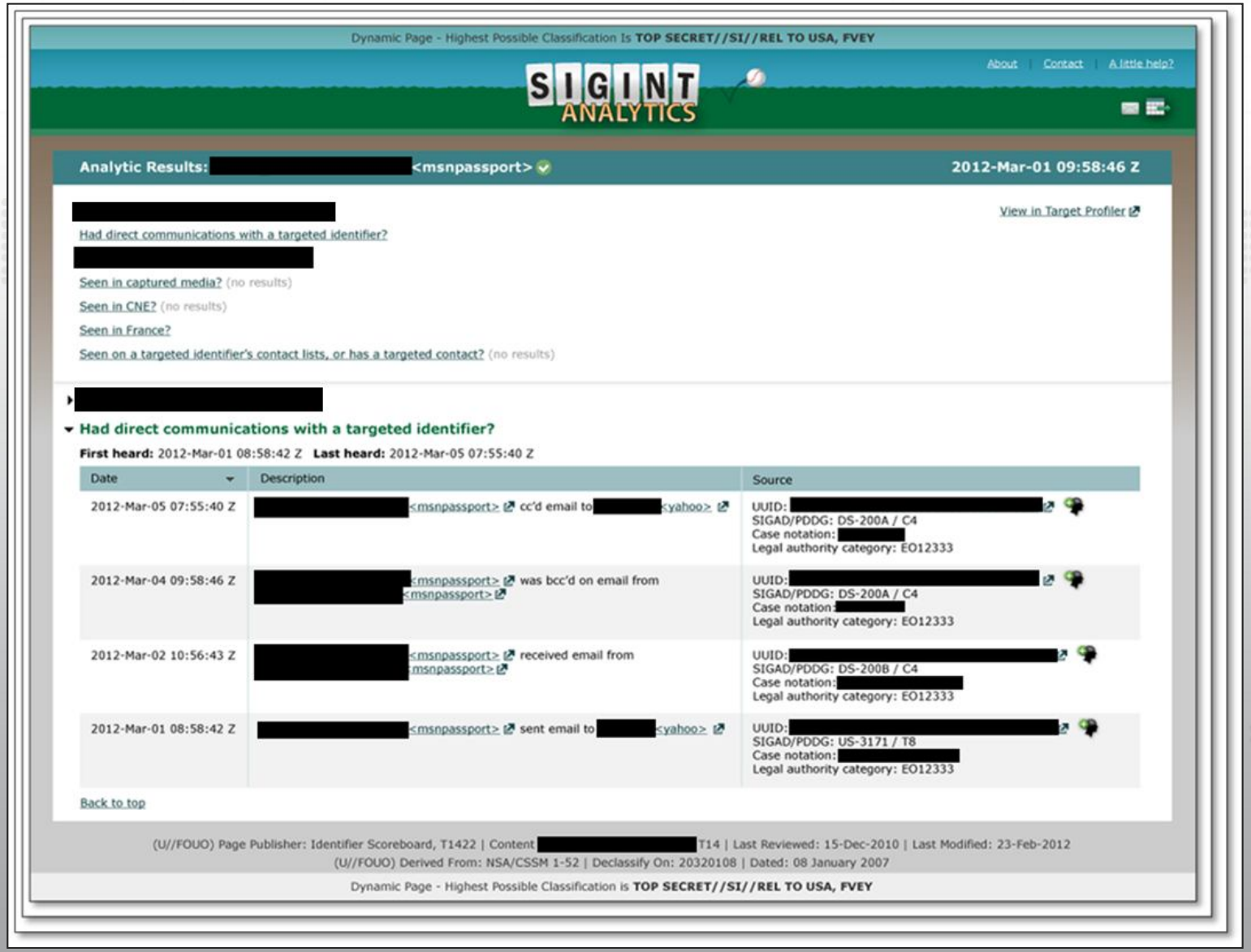


Normalized identifier	Positive Results	Direct Comms with Target?	Targeted Contact?	In Captured Media?	[redacted]	Se
[redacted]	2	•	n/a	n/a	n/a	
[redacted]	n/a					
[redacted]<msnpassport> View detailed analytic results	4	**Targets:** [redacted]<yahoo> TP [redacted]<facebookname> TP **First heard:** 25 Oct 2011 **Last heard:** 09 Mar 2012			[redacted] **First heard:** 03 Dec 2011 **Last heard:** 29 Feb 2012	[redacted]
[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		•			

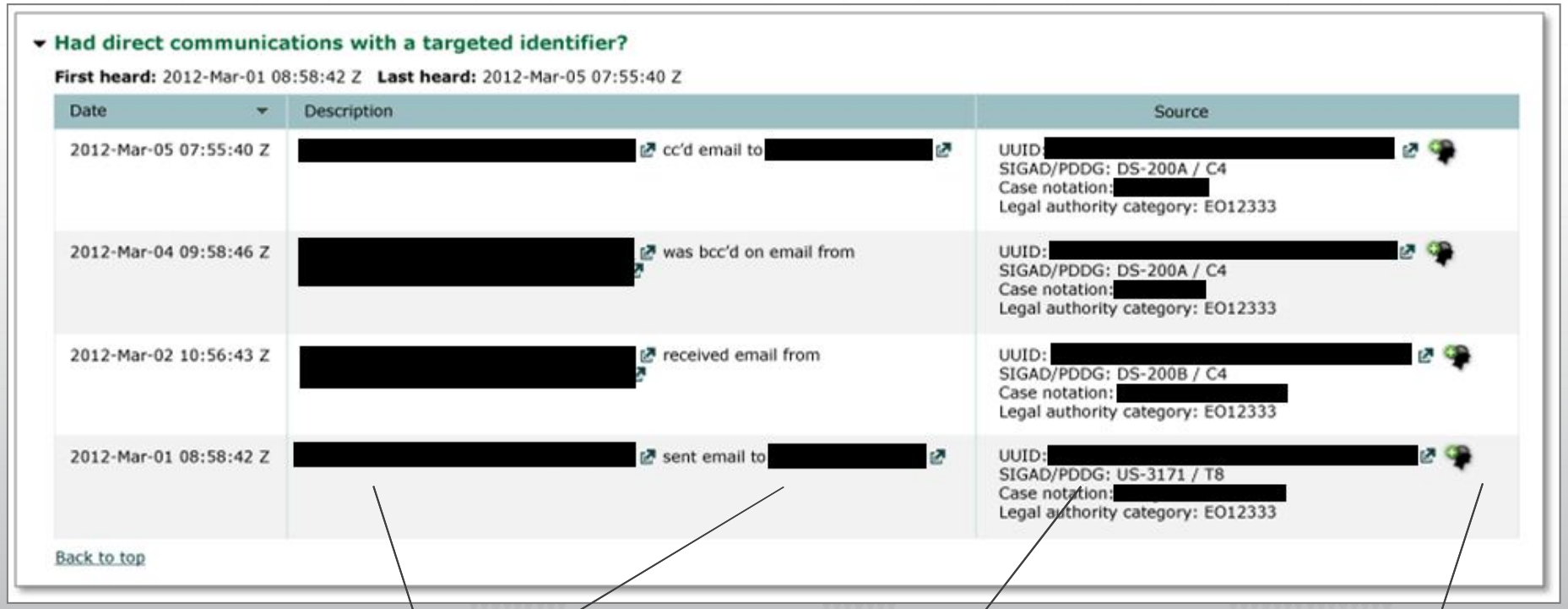
One column per ‘yes/no’ question

Quickly zero in on worthy leads

SIGINT Analytics Mode – Detailed View



SIGINT Analytics Mode – Detailed View



Go view target knowledge

Go view content

Add new knowledge

External links to guide next steps in analysis

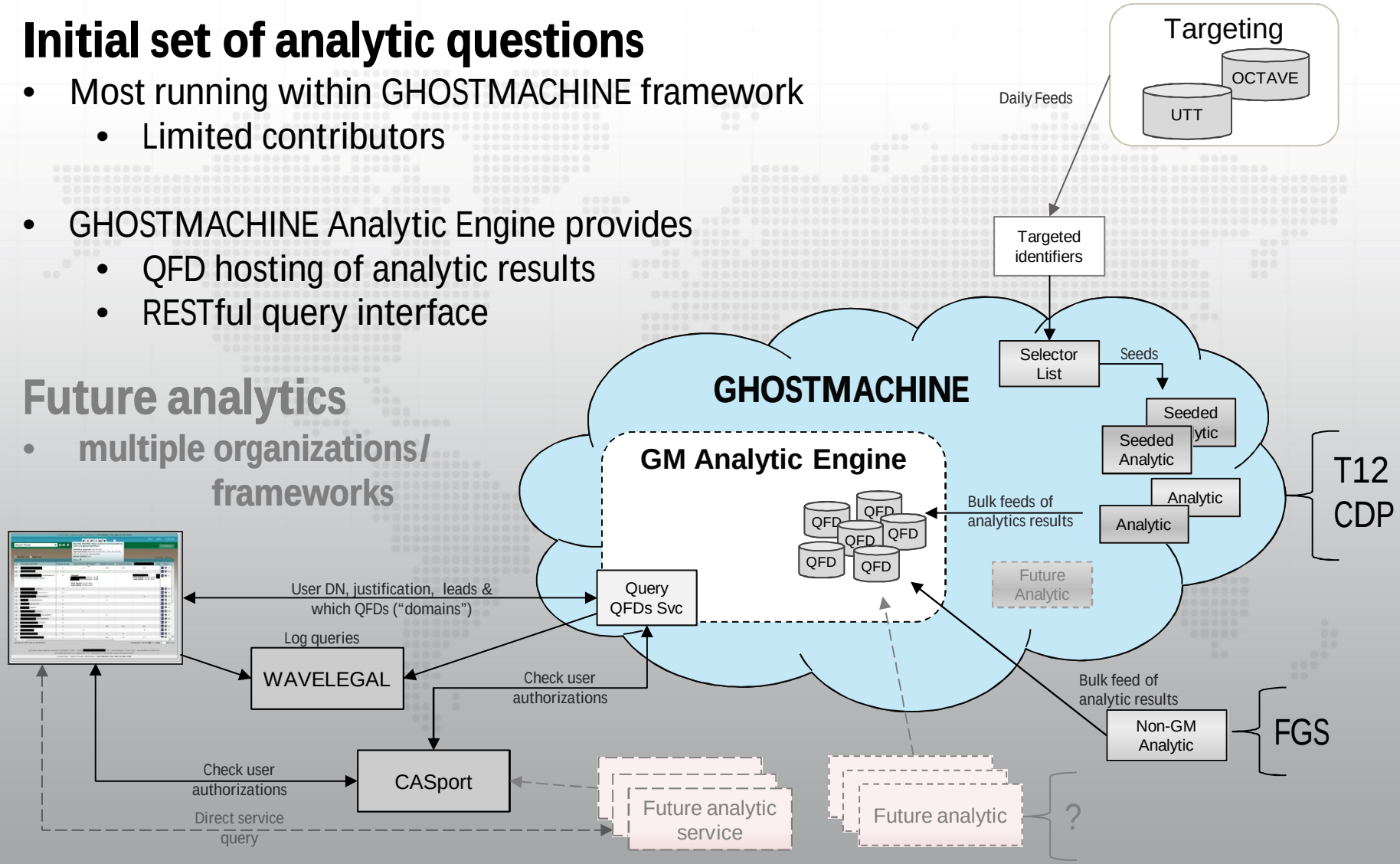
ECHOBASE Analytics Architecture

Initial set of analytic questions

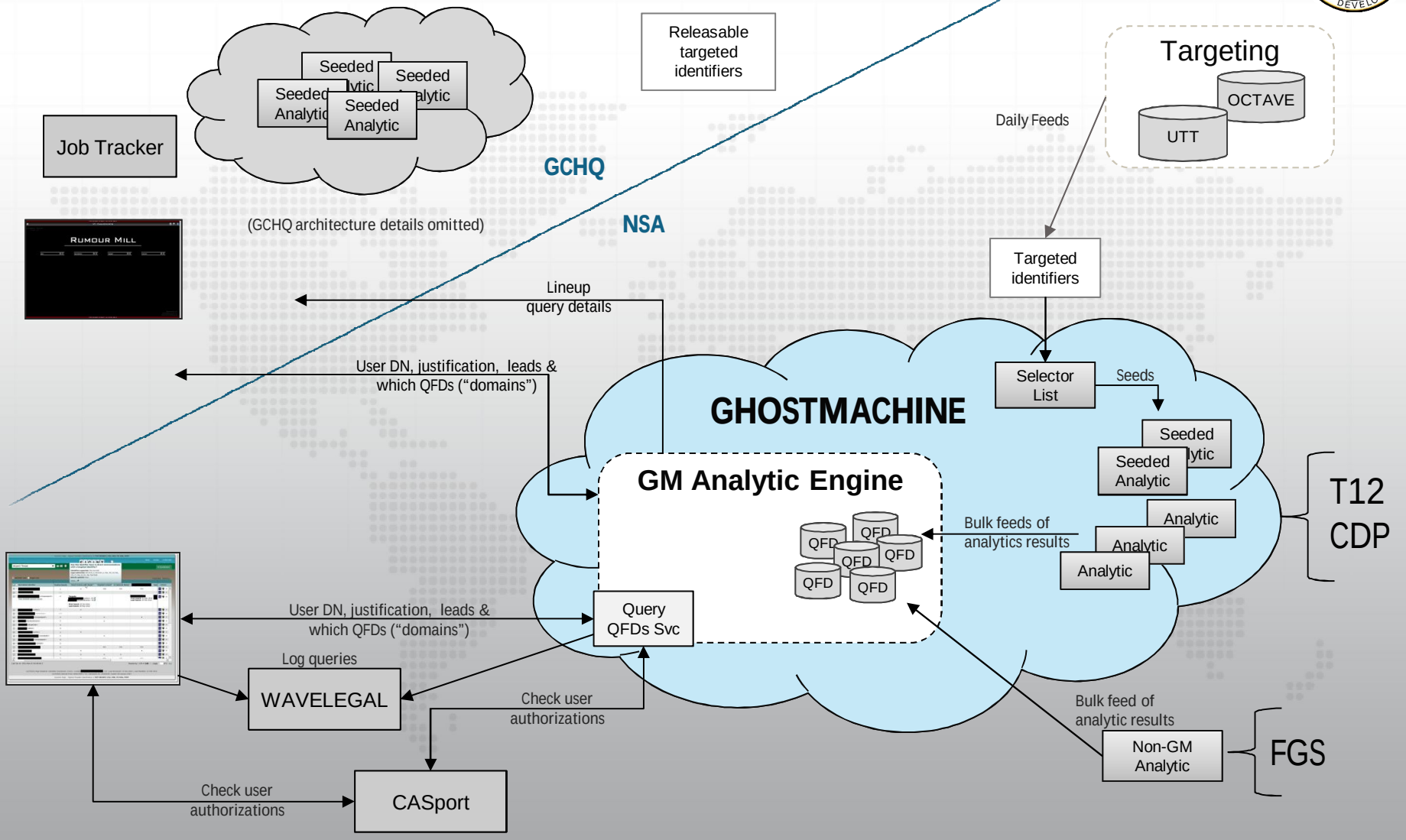
- Most running within GHOSTMACHINE framework
  - Limited contributors
- GHOSTMACHINE Analytic Engine provides
  - QFD hosting of analytic results
  - RESTful query interface

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 WikiInfo page:
  - [redacted]