Identifier Lead Triage
with ECHOBASE

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:

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seed List Provided to SIGDEV</td>
<td>Normalize and Expand Selectors</td>
<td>Foreignness and Compliance Check</td>
<td>SIGINT Queries on Selector activity and behavior attributes</td>
</tr>
</tbody>
</table>

Bulk enrichment of ‘SIGINT business knowledge’

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

- No Further Analysis Needed: 20%
- Definite Interest (Pri 1): 5%
- Possible Interest (Pri 2): 75%

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

![Pie chart showing interest levels]

- No Further Analysis Needed: 20%
- Low Interest (Pri 4): 25%
- Medium Interest (Pri 3): 35%
- High Interest (Pri 2): 15%
- Definite Interest (Pri 1): 5%
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

<table>
<thead>
<tr>
<th>Normalized Identifier</th>
<th>Positive Results</th>
<th>Direct Comm with Target?</th>
<th>Targeted Contact?</th>
<th>In Captured Media?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td></td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>&lt;msnpassword&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View detailed analytic results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;yahoo&gt;</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;emailAddr&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;msnpassword&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;facebookname&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;skypeUser&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;yahoo&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;emailAddr&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;emailAddr&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*First heard: 03 Dec 2011
*Last heard: 29 Feb 2012

One column per ‘yes/no’ question

Quickly zero in on worthy leads
**SIGINT Analytics Mode – Detailed View**

### Analytic 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-Mar-05 07:55:40 Z</td>
<td>was cc’d email to [redacted] [email] yahoo&gt;</td>
<td>[redacted] [ID: SIGD/PGDG: DS-200A / C4 Case number: [redacted] Legal authority category: [redacted]]</td>
</tr>
<tr>
<td>2012-Mar-04 09:58:46 Z</td>
<td>was bcc’d on email from [redacted] [email] msnpassport&gt;</td>
<td>[redacted] [ID: SIGD/PGDG: DS-200A / C4 Case number: [redacted] Legal authority category: [redacted]]</td>
</tr>
<tr>
<td>2012-Mar-02 10:56:43 Z</td>
<td>received email from [redacted] [email] msnpassport&gt;</td>
<td>[redacted] [ID: SIGD/PGDG: DS-200B / C4 Case number: [redacted] Legal authority category: [redacted]]</td>
</tr>
<tr>
<td>2012-Mar-01 08:58:42 Z</td>
<td>sent email to [redacted] [email] yahoo&gt;</td>
<td>[redacted] [ID: SIGD/PGDG: US-2171 / TB Case number: [redacted] Legal authority category: [redacted]]</td>
</tr>
</tbody>
</table>

### Additional Information

(U//FOUO) Page Publisher: Identifier Scoreboard, T1422 | Content T14 | Last Reviewed: 15-Dec-2010 | Last Modified: 23-Feb-2012
### SIGINT Analytics Mode – Detailed View

#### Had direct communications with a targeted identifier?

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-Mar-05 07:55:40 Z</td>
<td>cc’d email to</td>
<td>UUJD:</td>
</tr>
<tr>
<td>2012-Mar-04 09:56:46 Z</td>
<td>was bcc’d on email from</td>
<td>UUJD:</td>
</tr>
<tr>
<td>2012-Mar-02 10:56:43 Z</td>
<td>received email from</td>
<td>UUJD:</td>
</tr>
<tr>
<td>2012-Mar-01 08:58:42 Z</td>
<td>sent email to</td>
<td>UUJD:</td>
</tr>
</tbody>
</table>

**Back to top**

---

**External links to guide next steps in analysis**

Go view target knowledge  
Go view content  
Add new knowledge
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

---

**WAVELEGAL**
- User DN, justification, leads & which QFDs ("domains")
- Log queries
- Check user authorizations

**CASport**
- Check user authorizations
- Direct service query

**GM Analytic Engine**
- Query QFDs Svc

**GHOSTMACHINE**
- Bulk feeds of analytics results
- QFD hosting of analytic results
- RESTful query interface

**T12 CDP**
- Seeded Mic
- Seeded Analytic
- Analytic

**Targeting**
- OCTAVE
- UTT

**FGS**
- Future analytic
- Future analytic
- Future analytic
- Non-GM Analytic

---

**TOP SECRET//COMINT//REL TO USA, CAN, AUS, GBR, NZL**

11
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:
- ECHOBASE Alias:
- NSA WikiInfo page: