SOCIAL ANTHROPOID

SECRET STRAP1
What is Social Anthropoid?

- A converged comms database. It allows you to see when your targets have communicated:
  - via phone
  - over the internet
  - or using converged channels (e.g., sending e-mails from a phone or making voice calls over the internet).

SECRET STRAP1
WHAT ABOUT EXISTING COMMS DATABASES?

- When SOCIAL ANTHROPOID contains all the necessary data and has all the core functionality of the legacy tools, SOCIAL ANIMAL, REFORMER/HAUSTORIUM and SALAMANCA will be decommissioned.
Why?
- Scaling – huge volumes of events, existing systems are creaking.
- Convergence.
- Appropriate design.

But still need to:-
- Enrich
- Visualise
- Merge with NSA data sources
What data is in Social Anthropoid?

- All of Salamanca

  Social Animal

  Instant Messenger

  Webmail

  SIP and H323 VOIP, Yahoo Voice

  Blackberry

  MMS

  SMS

  GTP (GPRS Session set ups)

  SMTP, POP3 and IMAP

SECRET STRAP1
Search type

- Selector
- Selector Pair
- Locator (not)

Selector search

Saved queries

You have 1 saved queries.
Saved query functionality has been temporarily disabled.

- Queries will be automatically submitted to all instances of SOCIAL ANTHROPOID and SOCIAL ANIMAL.
- For bulk queries, enter multiple selectors (one per line).
- If allow wildcards is ticked, % is treated as a multi-character wildcard (e.g. paul will match paul@ics.uci.edu).
- Unlike other QFDs, _ and \ have no special meaning (to query for a literal % sign, use %)
- Updated: The system will automatically retrieve records containing the normalised version of your selector.

Relative Date

27-Jan-2011 10:49:01

Set Date

Miranda 20140
JIC Priority & Purpose 1st/1st
HRA Justification Testing

Filter results by matched selectors prior to display
Allow wildcards
Enable Selector Normalisation
Query active users only

Search period (optional):

Include Time

Lots of mixed selectors!

Date range - need start and end, relative dates

Saved queries

Multiple Results Tabs

Login screen

QUERY SCREEN
Your input terms matched 78 events from Sun, 08 Aug 2010 23:06:45 GMT to Fri, 21 Jan 2011 03:33:49 GMT.
You may restrict the selectors matching your input terms by selecting from the values below, prior to proceeding to your query results.

Select all  De-select all

- gmail.com (email_address) — 2 occurrences
- Gmail.com (Unknown) — 1 occurrences
- Hotmail.com (Unknown) — 1 occurrences
- Live.se (Owner) — 3 occurrences
- Live.se (Sender) — 5 occurrences
- Live.se (Unknown) — 33 occurrences

Optional

Filter results by matched selectors prior to display
Will be better with Broadoak!

Header contains key info:

- **Date**
- **Time**
- **Duration**
- **Tech universe**
- **Tech type**
- **Action**
- **Active user**
RESULTS: MORE METADATA

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be subject to other UK information legislation. Refer any FOIA queries to GCHQ or:  

Transferring data from

OTHER INFO IN QFD SPEAK

Hover over to display the tooltips for the metadata
**FILTERS, SUMMARISATION AND DRILL-DOWN SEARCHES**

**SOCIAL ANTHROPOID**

<table>
<thead>
<tr>
<th>User A role</th>
<th>User A type</th>
<th>User A raw value</th>
<th>User A display name</th>
<th>User B role</th>
<th>User B type</th>
<th>User B raw value</th>
<th>User B display name</th>
<th>User display name</th>
<th>Action type</th>
<th>Action</th>
<th>Locators</th>
</tr>
</thead>
</table>
|             |             |                  |                     |             |             |                  |                     |                   |             | unknown | unknown call
|             |             |                  |                     |             |             |                  |                     |                   |             |         | not available |

**GOOD SUMMARY OF TARGET BEHAVIOUR**

**SECRET STRAP1**
Quick Wins

AKA New things we can do in Social Anthropoid that we couldn’t do before
殇 Much more context in Social Anthropoid

SECRET STRAP1
There are 2 primary vectors for converged events:

- **GRX (GPRS Roaming exchange)** – uses GTP (GPRS Tunnelling Protocol).
- **CORE internet Collection** – leaky gateways.
Leaky gateways

**Social Anthropoid**

Logged in as:

More

Active user: UserA (AccountOwner) [MachineId] [X-huawei-IMSI]

Action: SendEmail, ActorContent: &<fi

Locators:

Source IPV4: Destination IPV4:

SRI: IRUKC03S_C0109 SigAd: UKC-113CV PDDG: HM

Source: BLACK HOLE filename: 201ûl024-0û0000-IRUKC035_C0109-done/con-ims.MS 2.log.gz Key: 4CC3F7989360FCü52-2D0990A000002B6 Plugin: A v4

Additional active user information:

User agent: SAMSUNG-GT-S5233A/L.0 SHV/PR/RS Jasmine/1.0 Next-generation SMH-HMS/1.2.8 profile/MIDP-2.1 configuration/CLDC-1.1

Additional meta-data:

Action: SendMail, ActorContext: Owner, Ctxt:

EventState: COMPLETE, Protocol: YahooWebmail:RouteInV4

Date/Time: 24-Oct-2010 06:10:16 — webmail event (yahoo), 5 selectors

More useful info
Full range of traffic types

Context rich action types

SECRET STRAP1
What features are we getting next?

- SCALE
- Geo including new filtering options
- Selector pairs query
- BROAD OAK ENRICHMENT
- Locator query
- Email domain query
- TDS
- DISPLAYNAMES

SECRET STRAP1
### Geo Inc. Filtering

#### Filter Criteria

- **Event type filtering**
- **Bearer filtering**
- **Geo filtering**

**Select all** | **De-select all**
--- | ---

<table>
<thead>
<tr>
<th>Geo filtering</th>
<th>Country</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Kazakhstan</td>
<td>1</td>
</tr>
<tr>
<td>✔️</td>
<td>Pakistan</td>
<td>39</td>
</tr>
<tr>
<td>✔️</td>
<td>United States</td>
<td>4</td>
</tr>
<tr>
<td>✔️</td>
<td>Unknown</td>
<td>371</td>
</tr>
</tbody>
</table>

#### Displayed Results

<table>
<thead>
<tr>
<th>Source IPV4</th>
<th>Destination IPV4</th>
<th>User A name</th>
<th>User A role</th>
<th>User A raw value</th>
<th>User A display name</th>
<th>User B name</th>
<th>User B role</th>
<th>User B raw value</th>
<th>User B display name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IPV4</td>
<td>Destination IPV4</td>
<td>User A name</td>
<td>User A role</td>
<td>User A raw value</td>
<td>User A display name</td>
<td>User B name</td>
<td>User B role</td>
<td>User B raw value</td>
<td>User B display name</td>
</tr>
</tbody>
</table>

**SECRET STRAP1**
Your input terms matched 14 events from Thu, 27 Jan 2011 09:12:33 GMT to Tue, 01 Feb 2011 16:42:20 GMT.
You may restrict the selectors matching your input terms by selecting from the values below, prior to proceeding to your query results. Any highlighted selectors are normalized versions of your original query seeds.

- Brandon.com.ua (Unknown) — 2 occurrences
- Brandon.com.ua (AccountOwner) — 6 occurrences
- Brandon.com.ua (AccountOwner) — 6 occurrences
- Brandon.com.ua (email_address) — 1 occurrences
- @Brandon.com.ua (AccountOwner) — 1 occurrences

Select all | De-select all

Save Query | Submit Query

SECRET STRAP1
Search type

- Selector
- Selector Pair
- Locator
- Email domain

Locator search

Saved queries

You have 1 saved queries.

- Queries will be automatically submitted to all instances of SOCIAL ANTHROPOID but NOT to SOCIAL ANIMAL.
- For bulk queries, enter multiple locators (one per line).
- If allow wildcards is ticked, * is treated as a multi-character wildcard.
  Unlike other QFDs, _ and \ have no special meaning (to query for a literal _ sign, uncheck 'allow wildcards' rather than 'escaping the wildcard.'
- By default, results will be returned in which your input locator appears in either the Source or Other locator column. Use the checkboxes below to change which of the source, other and destination columns you query.
- Selecting "Search all types" will return all matches regardless of the locator type.
  When "Search all types" is false, you must select at least one type. Locators have to match one of these types to be returned. You can only pick the types that are available for the database columns (source, destination and/or other) you have selected.

Locators:

Types to query:

- Cell-Global-Identifier
- Dest-IP-Address
- Dest-Point-Code
- Flight-Number
- INMARSAT-Service-

Search period (optional):

- Allow wildcards
- Search all types
- Target Enrichment

Query for source locators
Query for other source locators
Query for destination locators

Target Enrichment

Miranda

JIC Priority & Purpose

HRA Justification

testing

Save Query
Submit Query
<table>
<thead>
<tr>
<th>Display Name Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary of all selectors with display names within this result set.</td>
</tr>
</tbody>
</table>

- service@youtube.com (Unknown)
  YouTube Service — 1 occurrences
- muslimaid@gator.cem13.co.uk (Unknown)
  Muslim Aid — 2 occurrences
- shotmail.com (Owner)
  Shotmail.com — 248 occurrences
- hotmail.com (Unknown)
  hotmail.com — 1 occurrences
- hotmail.com (Unknown)
  hotmail.com — 1 occurrences
- hotmail.com (AccountOwner)
  hotmail.com — 21 occurrences
- hotmail.com (Unknown)
  hotmail.com — 1 occurrences
- hotmail.com (Unknown)
  hotmail.com — 1 occurrences
- hotmail.com (Unknown)

**TDS generation**

**Work on a profile/summary query**

**SECRET STRAP1**
SECRET STRAP1
Roll out plan.

- Tranche 1 – WC 24 Jan 100 users
- Tranche 2 – WC 31 Jan 260 users
- Tranche 3 – WC 7 Feb 100 users
- Tranche 4 – WC 14 Feb Mop up users

- Rollout to SALAMANCA users will follow
Contacts

Senior Users:

Business Change:

SECRET STRAP1
Questions?