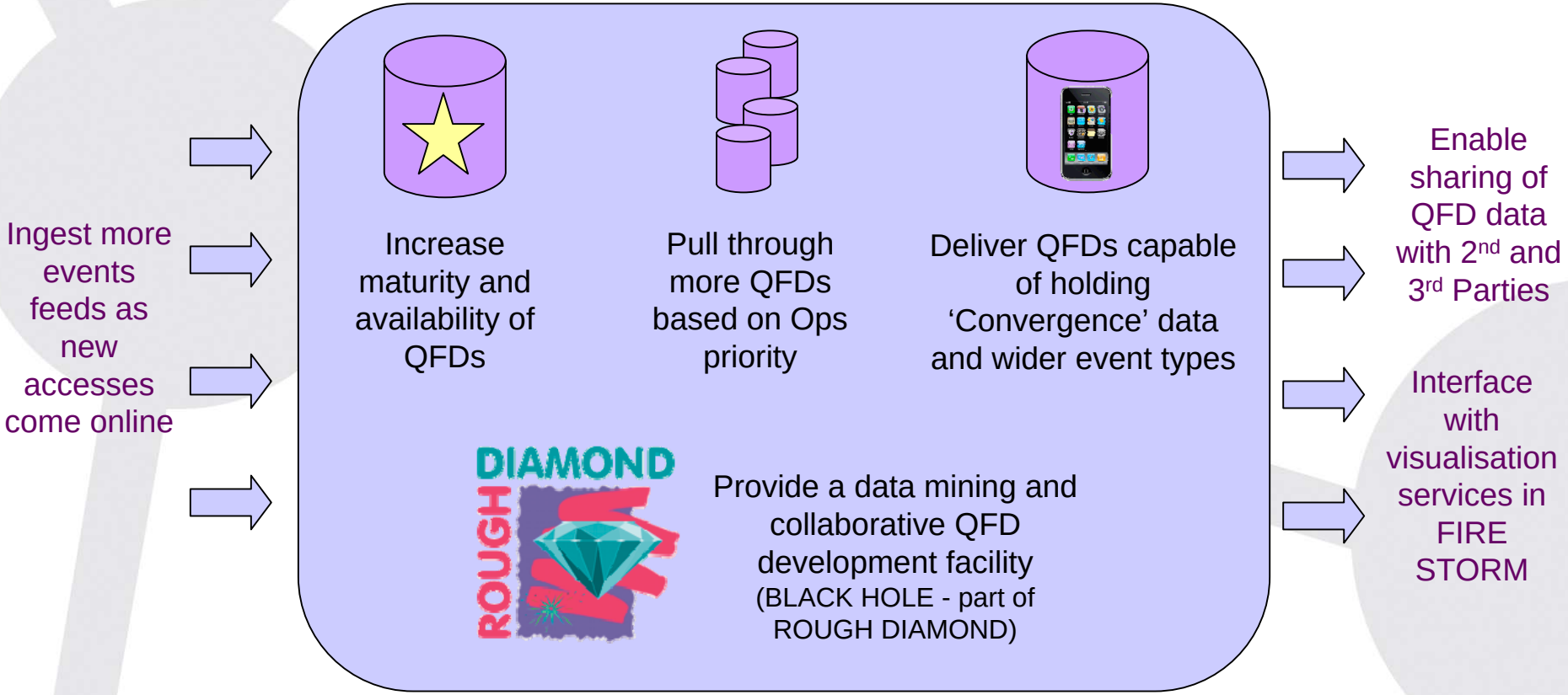
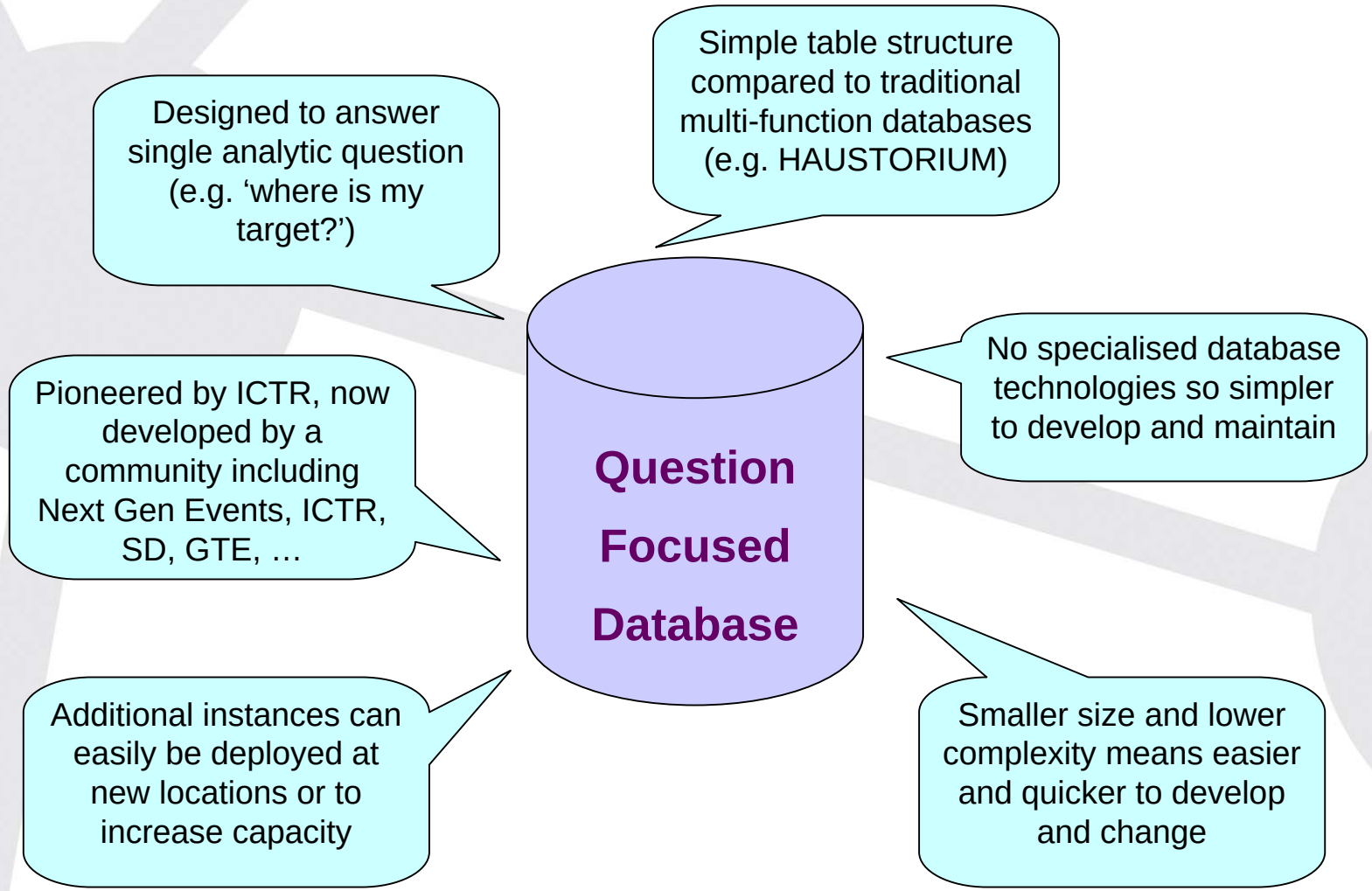
NEXT GENERATION events

Scope and Aims



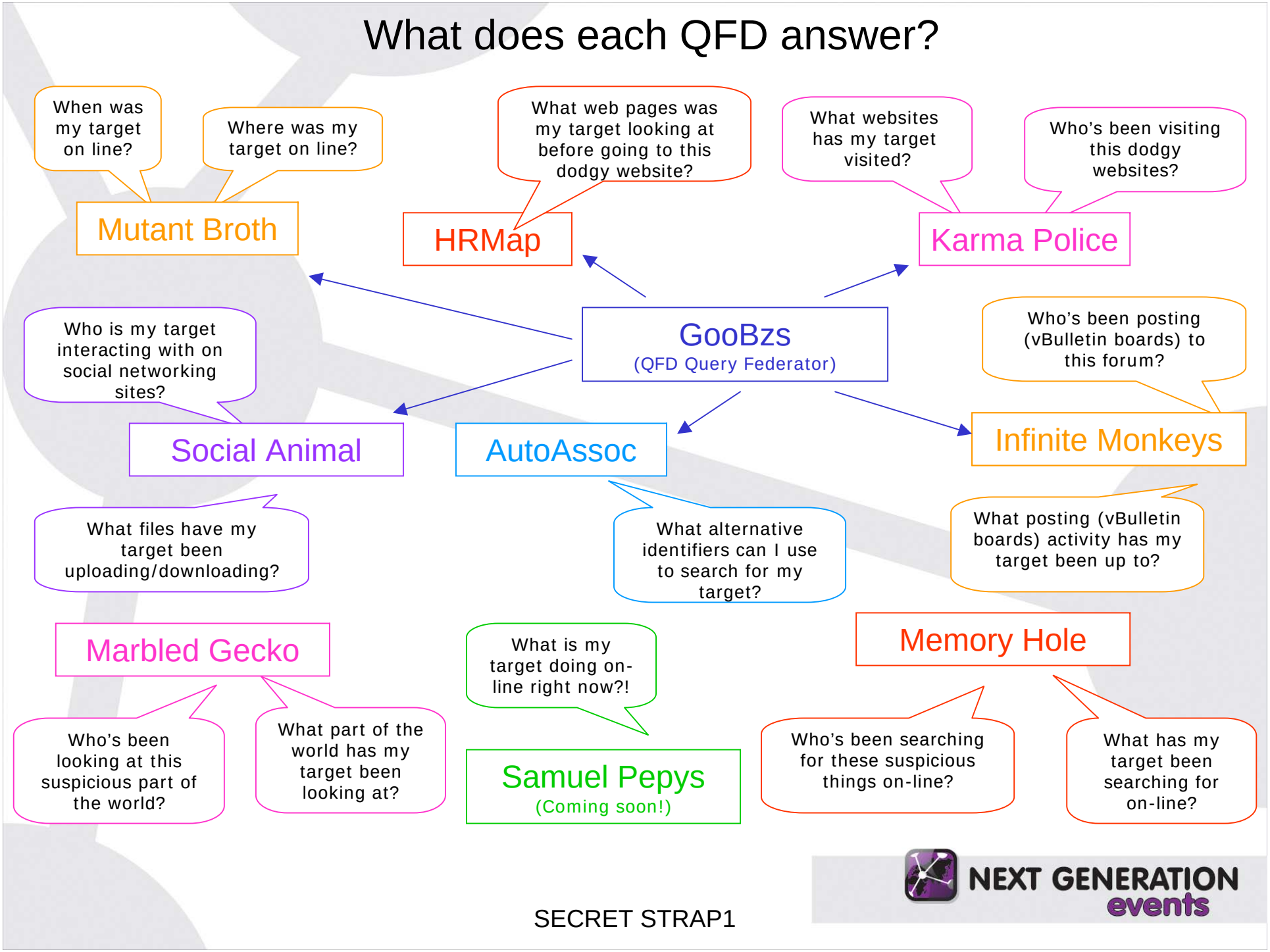
NEXT GENERATION events

What is a QFD?



NEXT GENERATION events

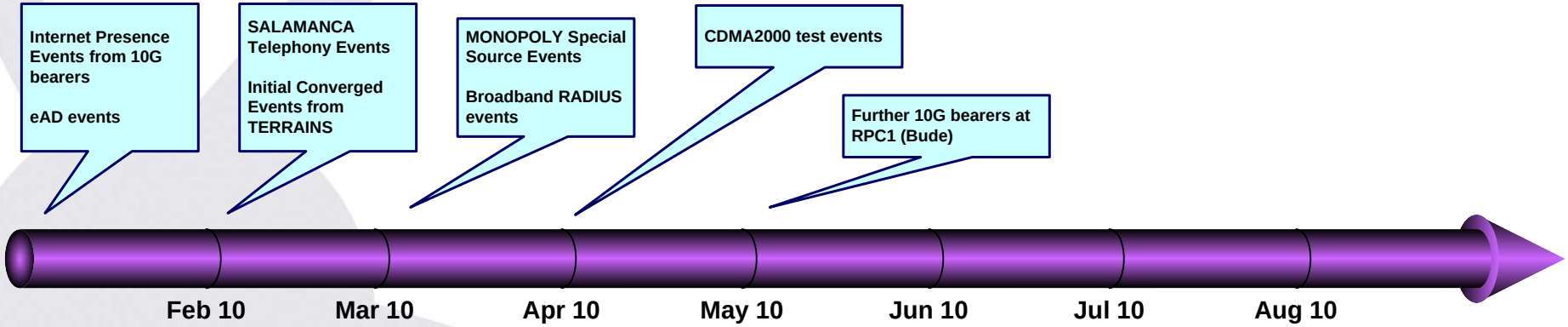
What does each QFD answer?



SECRET STRAP1

NEXT GENERATION events

Ingest roadmap



Trial part 1 - MUTANT BROTH, INFINITE MONKEYS, HRMAP, MEMORY HOLE from mobile tunnels

Experiment — Explore — Deployed across CPC and RPC1

Trial part 2 - MMS, Blackberry, Google Maps, mobile Hotmail, mobile Gmail from mobile tunnels

Explore — Deployed across CPC and RPC1

TPS are working with the NGE Project and SMO Mobile theme to produce internet presence and application usage events from within mobile phone 'tunnels' in internet bearers. These will be trialed before full operational rollout

Trial part 3 - Hotmail, Gmail, mail RU, Yahoo webmail from internet bearers

Experiment — Explore — Deployed across CPC and RPC1

Trial part 4 - Windows Live IM, Yahoo Mail, SIP from internet bearers

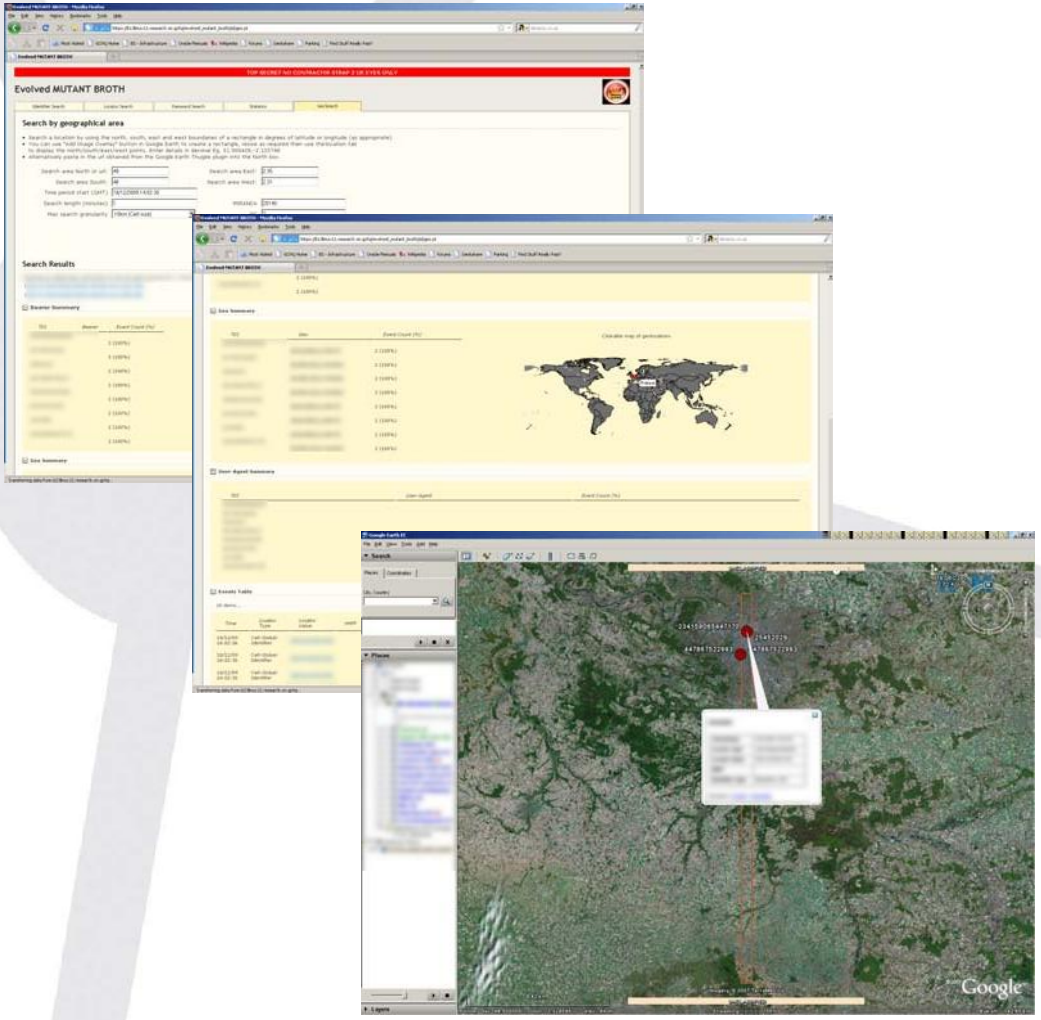
Explore — Deployed across CPC and RPC1

'QFD style' events will also be produced for types of event traditionally fed into the older HAUSTORIUM and HARBOUR PILOT databases

NEXT GENERATION events

SECRET STRAP1

Convergence QFDs



Screenshots from evolved MUTANT BROTH web interface, and an export of it's data to Google Earth

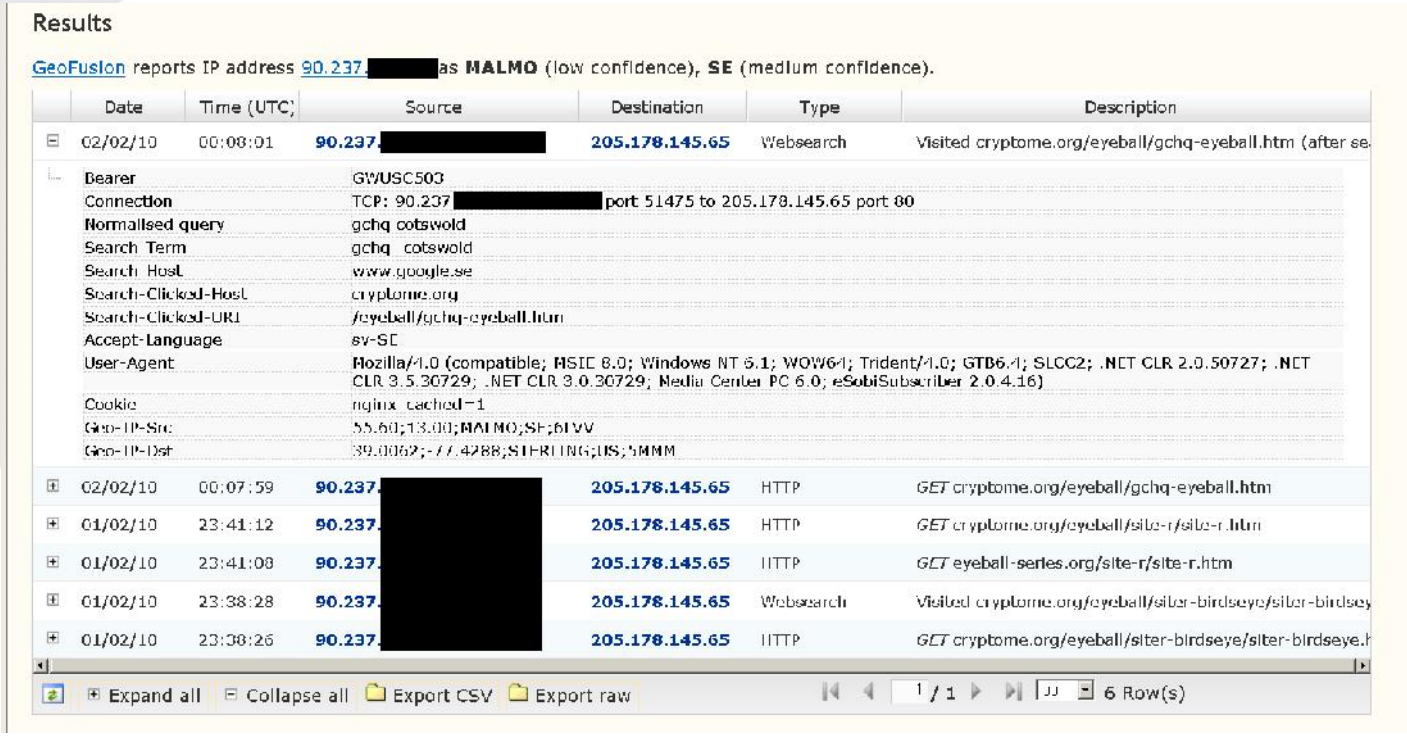
This major thread of work will:

- Store events where internet applications are accessed from a mobile device
- Allow analysts to relate mobile device identifiers to internet identifiers such as email addresses
- Enable QFDs to store other more diverse event types, such as telephony events (currently SALAMANCA), and email events (currently HAUSTORIUM / HARBOUR PILOT)
- Interface to LOOKING GLASS visualisation coming soon (in FIRE STORM work package)

NEXT GENERATION events

SAMUEL PEPYS QFD

Purpose: Provide a near-real-time diarisation of any IP address



Results

GeoFusion reports IP address 90.237.[redacted] as **MALMO** (low confidence), **SE** (medium confidence).

Date	Time (UTC)	Source	Destination	Type	Description
02/02/10	00:08:01	90.237.[redacted]	205.178.145.65	Websearch	Visited cryptome.org/eyeball/gchq-eyeball.htm (after se

Bearer	GWUSC503
Connection	TCP: 90.237.[redacted] port 51475 to 205.178.145.65 port 80
Normalised query	gchq cotswold
Search Term	gchq cotswold
Search Host	www.google.se
Search-Clicked-Host	cryptome.org
Search-Clicked-URI	/eyeball/gchq-eyeball.htm
Accept-Language	sv-SE
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; GTB6.4; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; eSobiSubscriber 2.0.4.16)
Cookie	nginx_cached=1
Geo-IP-Src	55.60;13.00;MALMO;SE;61VV
Geo-IP-Dst	39.0062;-77.4288;STERLING;US;DMMM

02/02/10	00:07:59	90.237.[redacted]	205.178.145.65	HTTP	*GET* cryptome.org/eyeball/gchq-eyeball.htm
01/02/10	23:41:12	90.237.[redacted]	205.178.145.65	HTTP	*GET* cryptome.org/eyeball/site-r/site-r.htm
01/02/10	23:41:08	90.237.[redacted]	205.178.145.65	HTTP	*GET* eyeball-series.org/site-r/site-r.htm
01/02/10	23:38:28	90.237.[redacted]	205.178.145.65	Websearch	Visited cryptome.org/eyeball/siter-birdseye/siter-birdsey
01/02/10	23:38:26	90.237.[redacted]	205.178.145.65	HTTP	*GET* cryptome.org/eyeball/siter-birdseye/siter-birdseye.h

Expand all | Collapse all | Export CSV | Export raw | 1 / 1 | 6 Row(s)

Prototyped by ICTR – Currently being pulled through by ROCK RIDGE, will be scaled to full 10G volumes by May 2010

BLACK HOLE

What is BLACK HOLE?

- A flat file store housing all data from a wide range of feeds (events and content)
- Provides a set of tools for accessing that data.
- Intended to be the source of events (and limited content) for the development of new QFDs and analytics.
- Contains a rolling 6 months retention
- Part of ROUGH DIAMOND

What does it enable?

- New QFDs to be rapidly prototyped, then to be added to the operational QFD suite
- Trialling of new bulk analysis ideas
- New sources of data to be introduced quickly into existing QFDs.
- Users to look for particular patterns and behaviours (target discovery)
- TR, GTAC and GTE access to more data for research purposes, which may not be QFD related.

User Feedback

'Absolutely FABULOUS well done '
(Iain Lobban, ref SUPERDRAKE reporting)

'its amazing to see how the pace of delivery in TDB has increased and I have been impressed by your responsiveness to customer needs. '
([redacted],Senior User)

'Almost exactly a year ago I set you the challenge of delivering an upscaled massive events capability … in order to support Internet Operations being conducted by GCHQ. Through your stripy team working on BLAZING SADDLES, BLUESHIFT and SUPPORTING INO you successfully met this challenge and delivered us a significant new capability in July.'
([redacted], Deputy Director Cyber Operations)

'It's working flawlessly'
(analyst, ref BLACK HOLE)

'Bloody awesome'
(analyst, ref SUPERDRAKE QFD)

NEXT GENERATION events