BLACK HOLE ANALYTICS

███████████████████████████████████████!

ADD/SD briefing, September 2009

Contents

- Describe the new breed of C2C tools developed in Applied Research (TR)

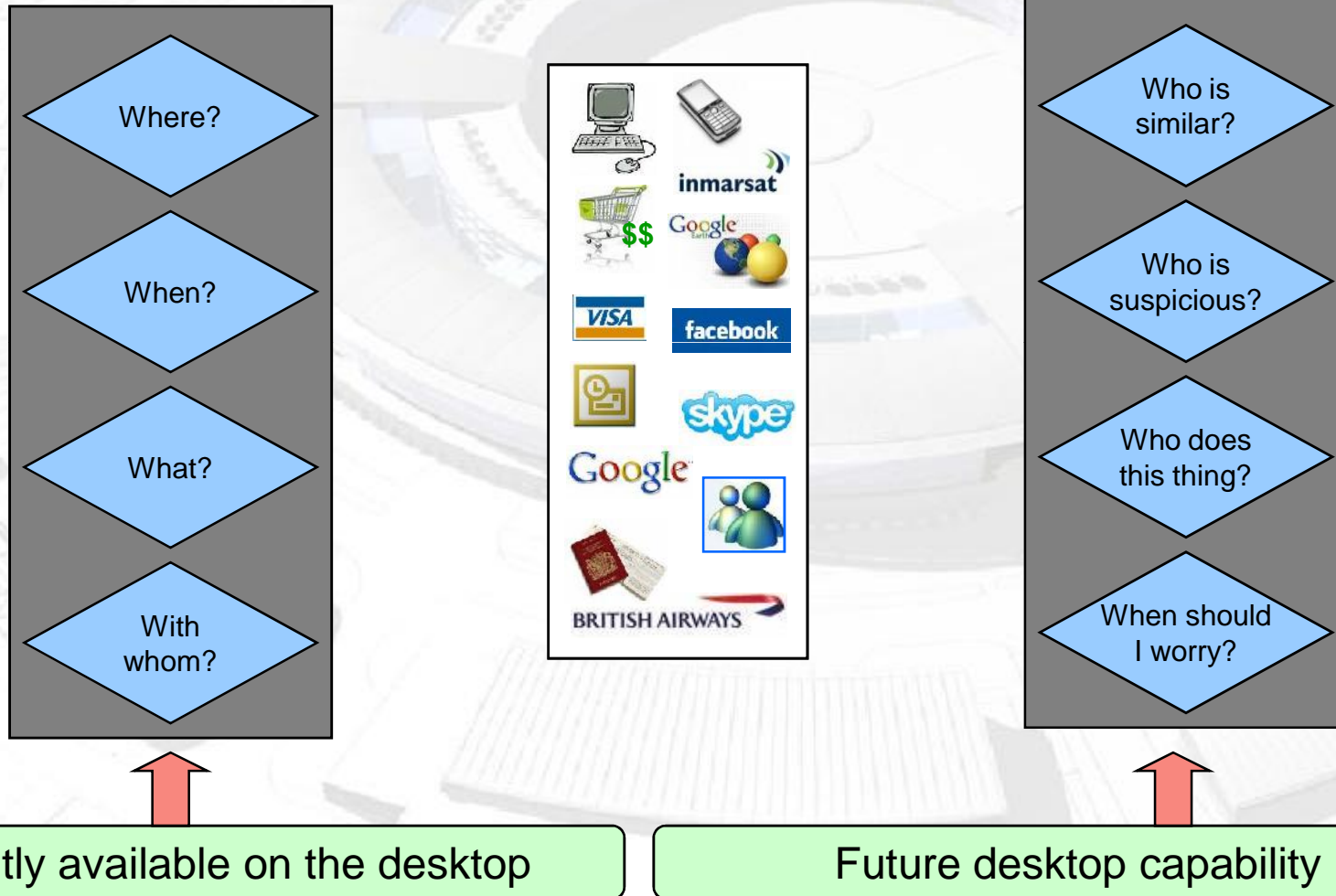- Scaling them up through the Next Generation Events (NGE) project

GTAC

Next Generation Events Roadmap

Convergence 1

~8 x 10g

Cloud upscale

~50 x 10g

Internet Profiling 2

~200 x 10g

July
2009

Mar
2011

Looking Glass deliveries

Looking Glass deliveries

Internet
Profiling 1

~80 x 10g
~260 experts

Capability development
(including eA)

Large-scale contact
chaining

Data mining and
profiling

New technologies (particularly from JCE) incorporated into solution as they are de-risked / proven

NGE Analytical Capabilities

Where?

When?

What?

With whom?

Who is similar?

Who is suspicious?

Who does this thing?

When should I worry?

Currently available on the desktop

Future desktop capability
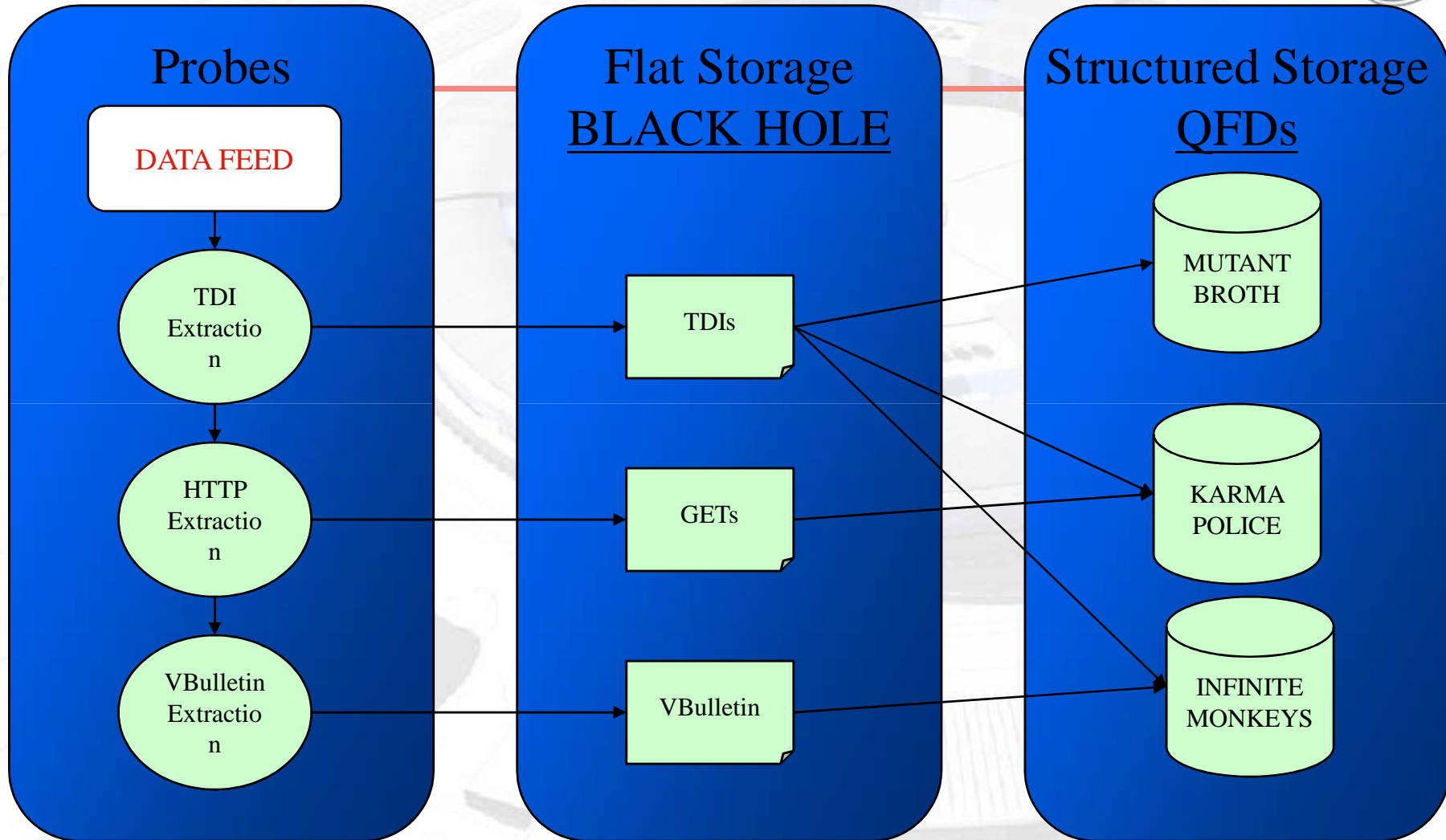
Some useful definitions

- Presence Event
- Describes that an identifier was online, on an IP address, at a point in time.
- Simple, atomic element.
- Can be very easily developed so are very diverse
- Very useful!

- TDI = Target Description Identifier
- Has a type, eg Yahoo-Y-Cookie
- And a value, eg tom123@yahoo

- GTDI = Generic Target Detection Identifier
- Expands the TDI concept to telephony e.g. A GSM location update message

Some more definitions

- BLACK HOLE: The large flat file storage where all the data sits
- After initial processing, and before being manipulated and correlated and loaded into the QFD database tables

- QFD: Question Focused Dataset (Database)
- One for each tool: MUTANT BROTH, AUTO ASSOC etc

Probes

DATA FEED

TDI Extraction

HTTP Extraction

VBulletin Extraction

Flat Storage
BLACK HOLE

TDIs

GETs

VBulletin

Structured Storage
QFDs

MUTANT BROTH

KARMA POLICE

INFINITE MONKEYS

QFD desktop…so far…

- Enables analysts to:

  - Create a profile of a target's online activities (Mutant Broth)

  - Find other identifiers for a target (Auto Assoc)

  - Create a social network (Social Animal)

  - Investigate websites or web forums of interest (Karma Police, Infinite Monkeys, HRMAP)

  - Find out who has been searching the web and for what (Memory Hole)

  - Find out who has been looking at what on Google Earth (Marbled Gecko)

Converged QFD desktop…by Dec…

- Enables analysts to:

  - Create a profile of a target's online activities alongside telephony (Evolved Mutant Broth)

  - Find alternative identifiers across telephony and the internet (Hard Assoc)

  - Create a social network including telephony (Evolved Social Animal)

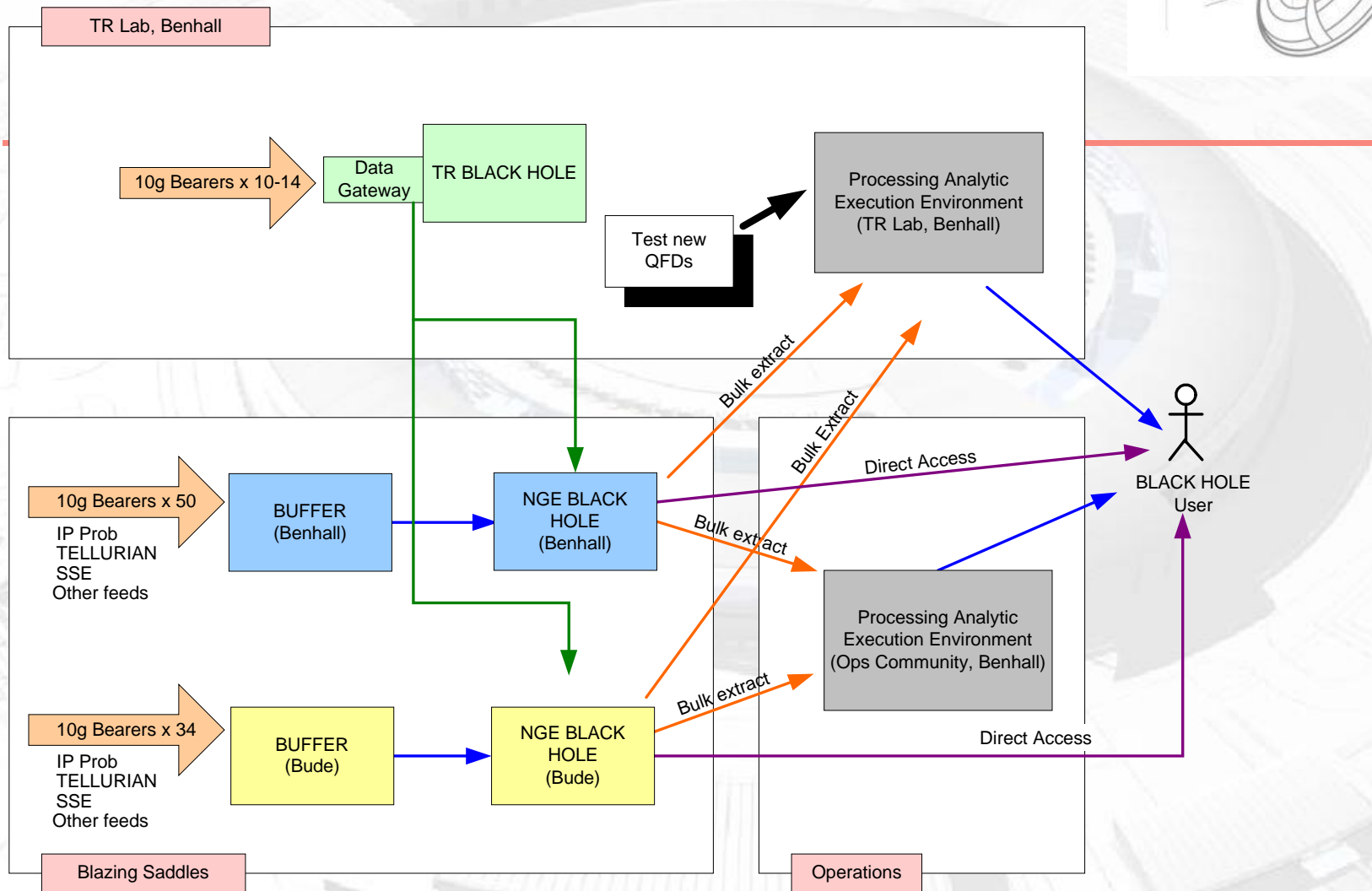 - Find out what has been happening in real time (Samuel Pepys)

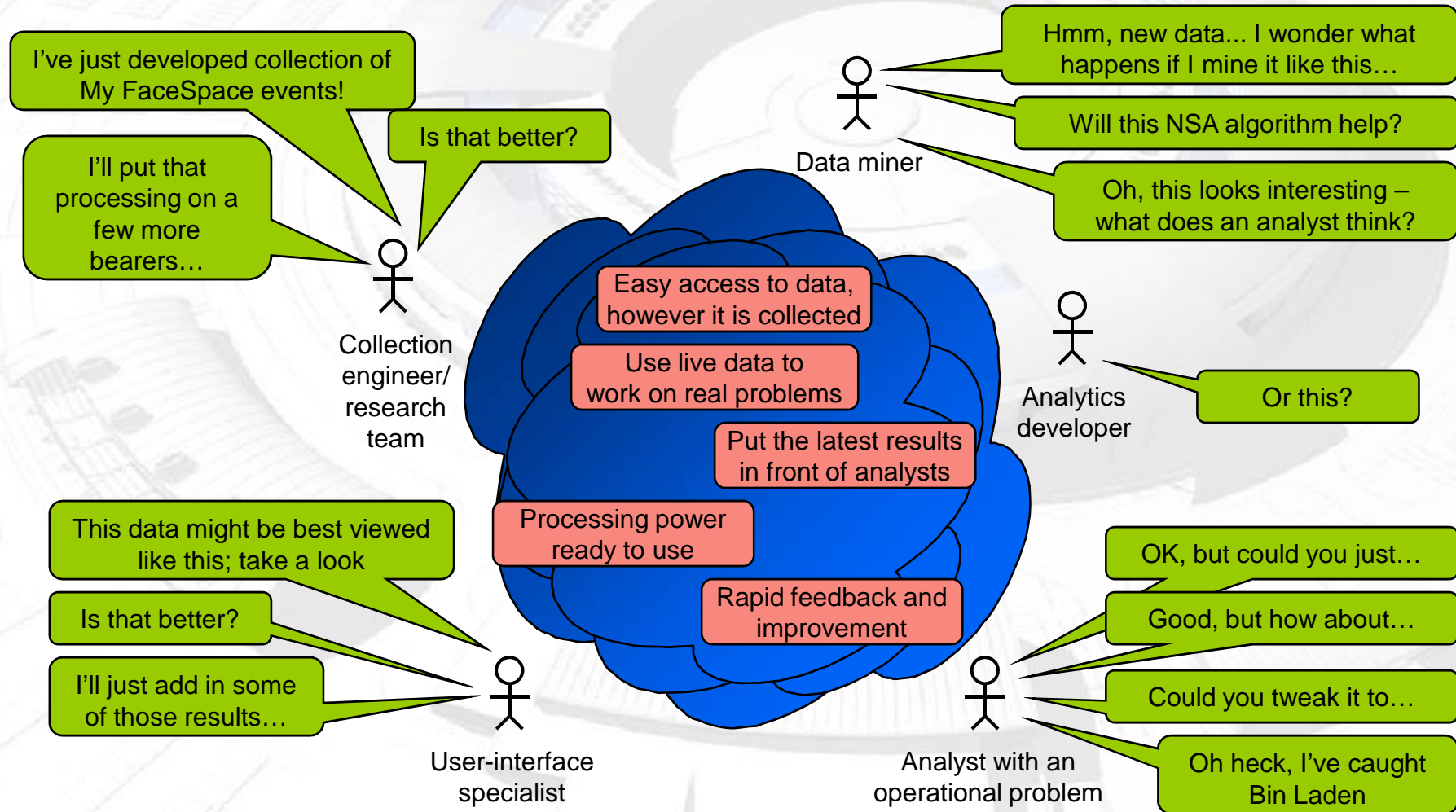 All available on the desktop via Looking Glass plug-ins and Web GUIs

Success story – TSS2 Nocon

- Slides removed – contact ███████████████ for full version
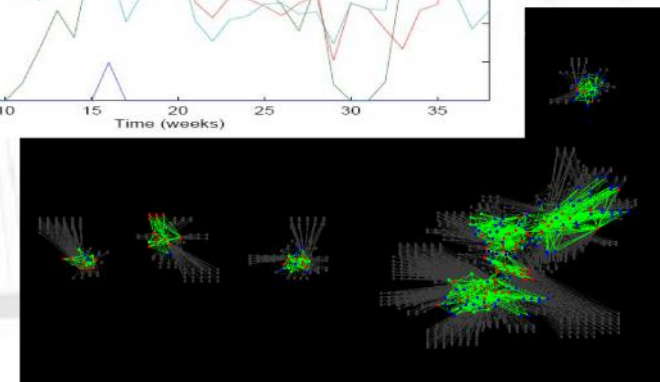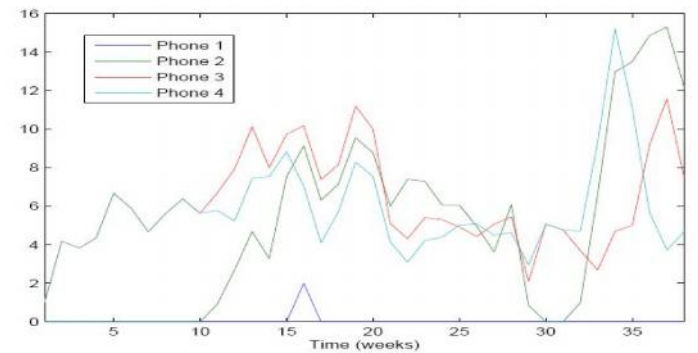
Data Mining at scale

- Experiments with Cloud ongoing to enable analysts to request and run MOAGs (large TNN graphs) from the desktop

- Distillery will enable analysts to spot real time changes to the data at scale (e.g. detection of impossible travel)

- Joint Collaboration Environment (Innov8) – trialling running of large scale analytics using both GCHQ and NSA data

Future Implications

- We shall be able to:

  - easily monitor changes in our targets' profiles and networks
  - develop and trial new capabilities using real life analytical experiments
  - respond quickly in a crisis

Questions?

/BLAZING_SADDLES

/NGE_BLACK_HOLE