BLACK HOLE ANALYTICS

[redacted]!

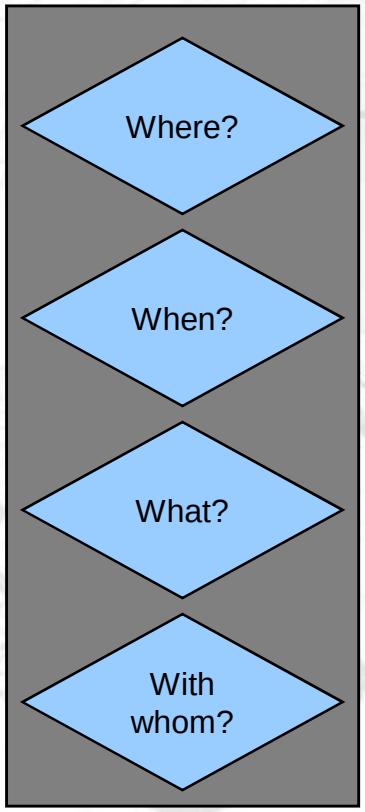
ADD/SD briefing, September 2009

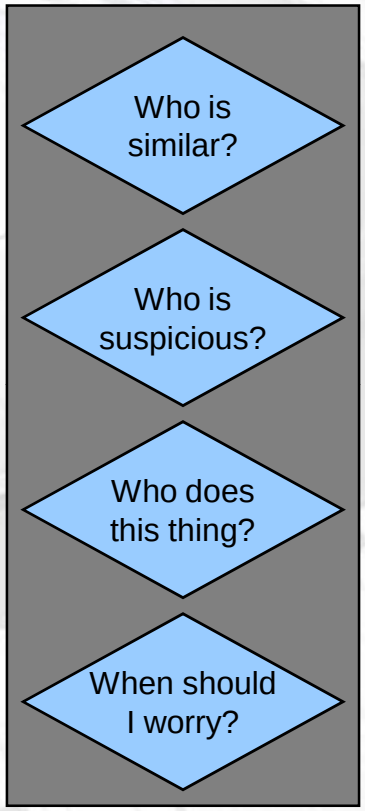
Contents

- Describe the new breed of C2C tools developed in Applied Research (TR)
- Scaling them up through the Next Generation Events (NGE) project

Next Generation Events Roadmap

NGE Analytical Capabilities





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!

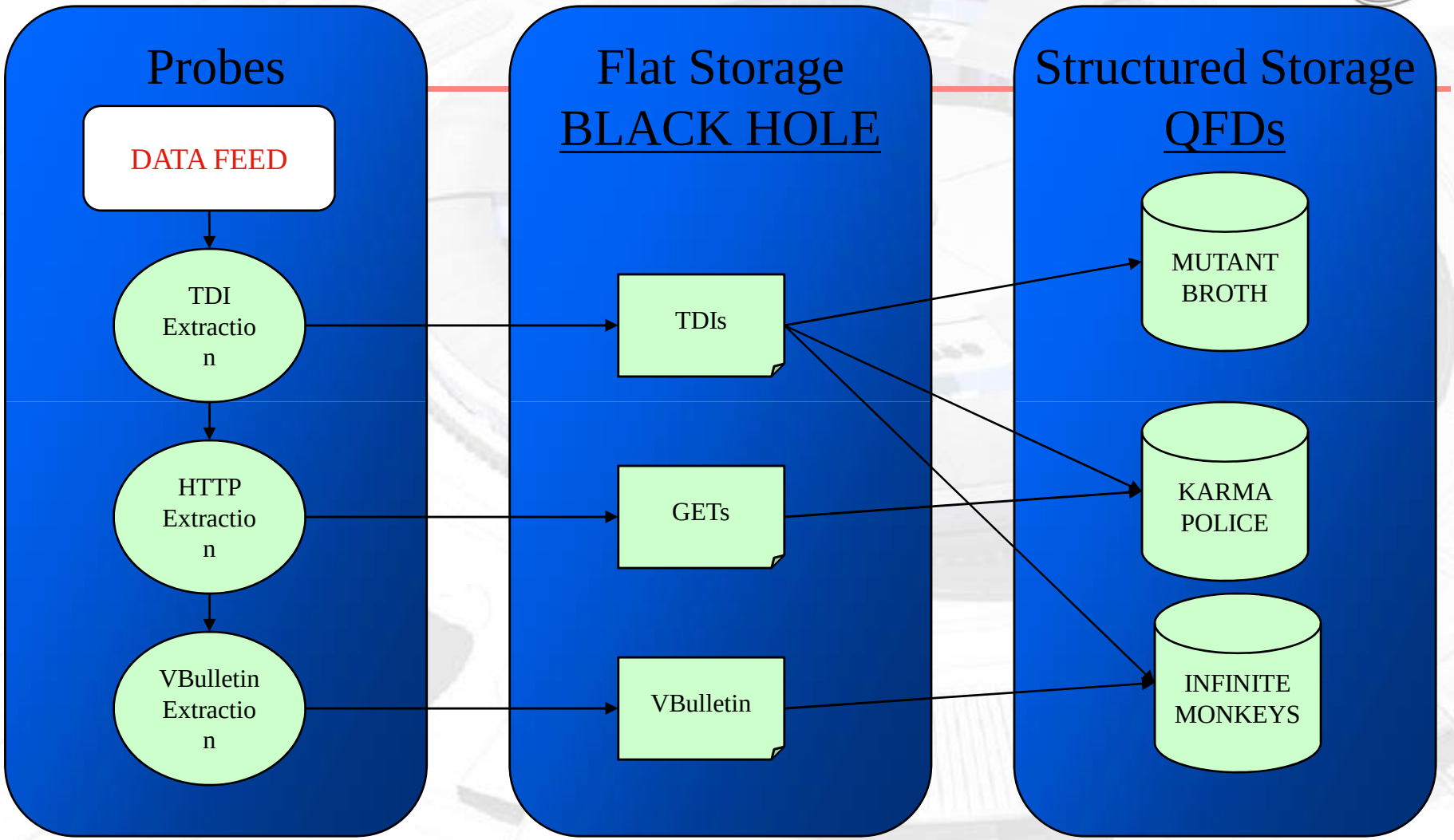
- TDI = Target Description Identifier
- Has a type, eg Yahoo-Y-Cookie
- And a value, eg tom123@yahoo

- 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



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)

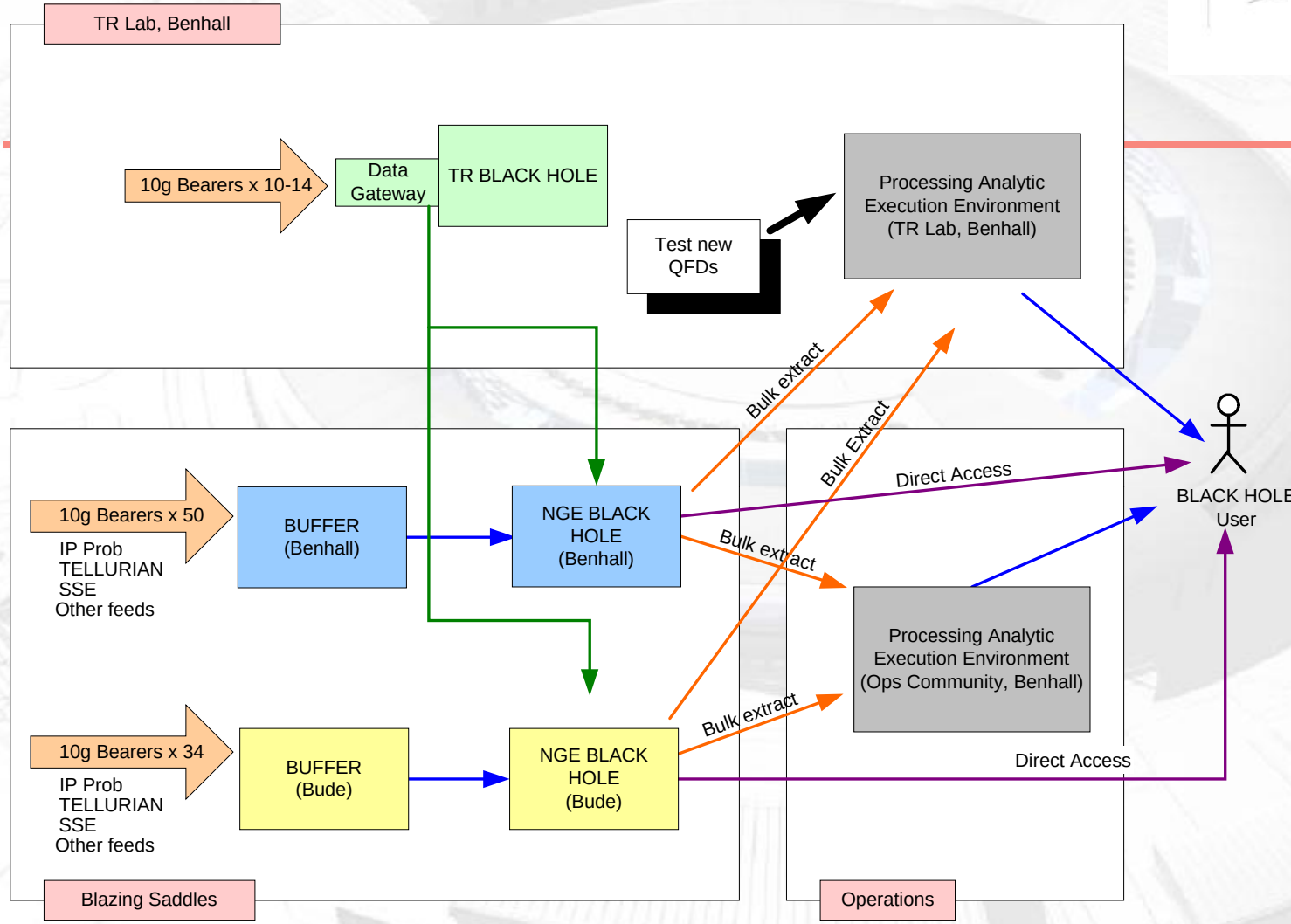
Converged QFD desktop...by Dec...

- 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)

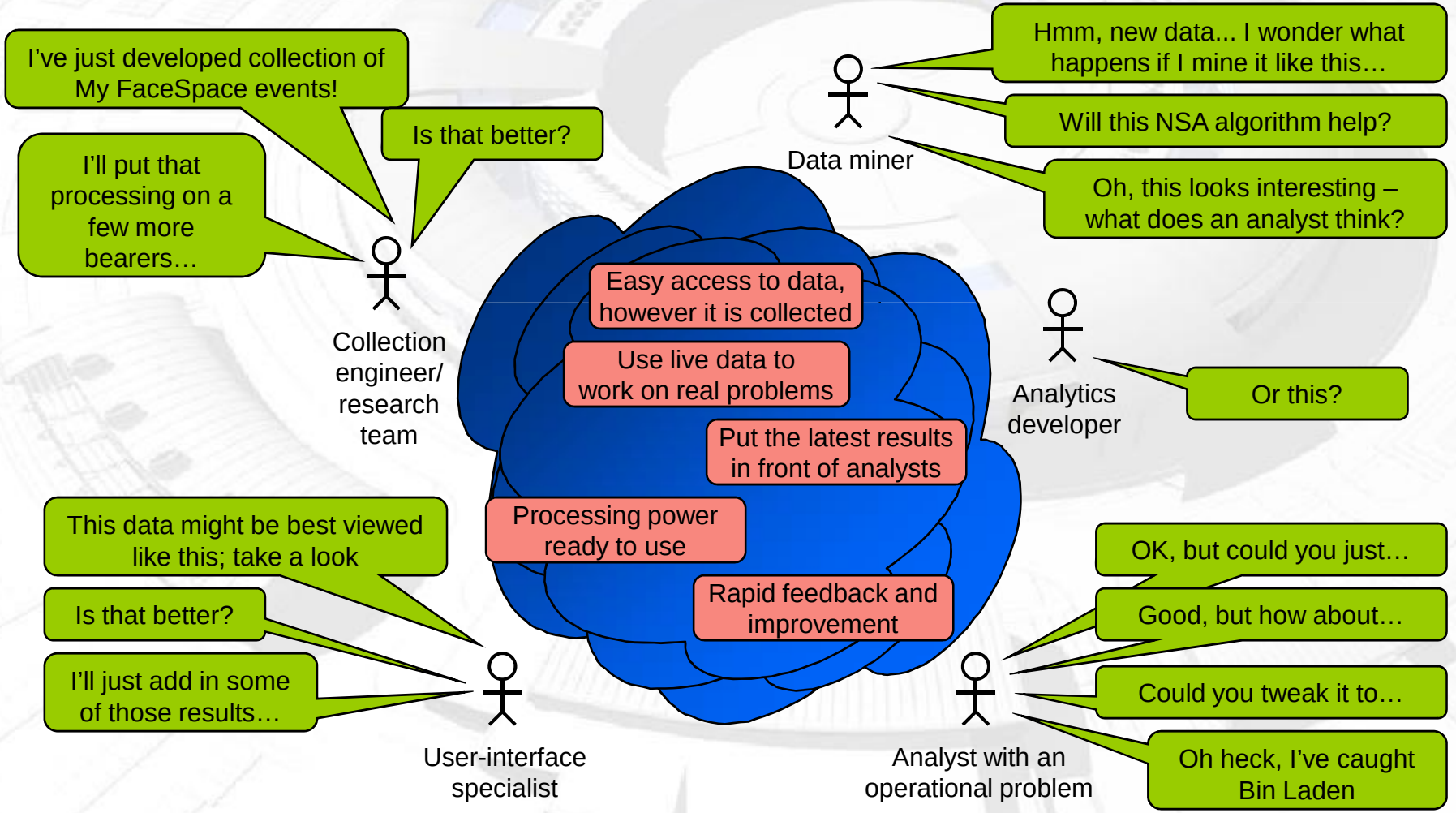
All available on the desktop via Looking Glass plug-ins and Web GUIs

Success story – TSS2 Nocon

- Slides removed – contact [redacted] for full version

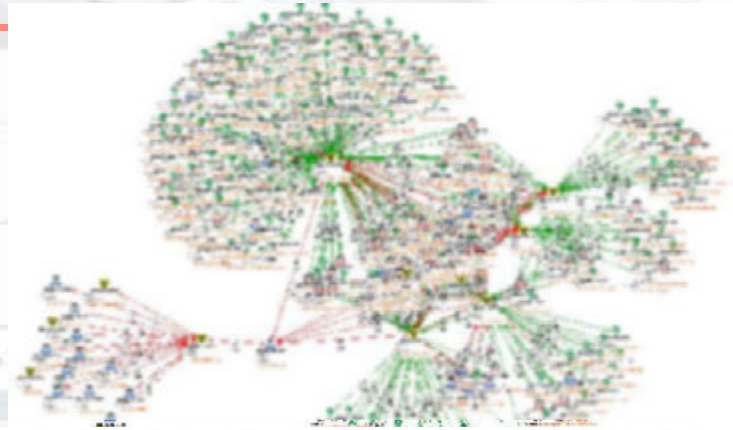


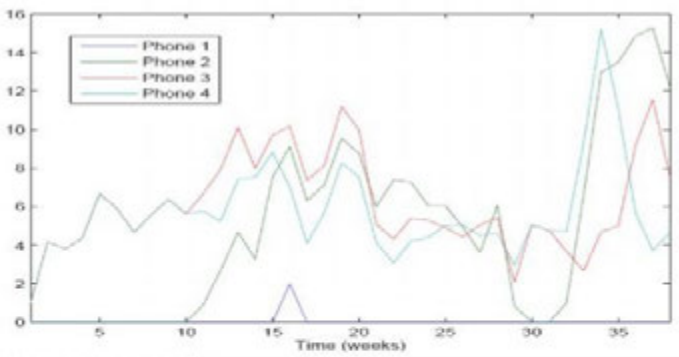
Capability Dev Workspace

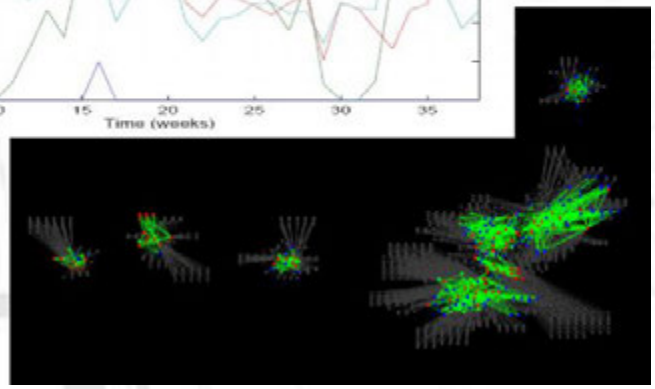


Data Mining at scale

- 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?

[redacted]/BLAZING_SADDLES

/NGE_BLACK_HOLE