

UK SECRET

The maximum [classification](#) allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to [report inappropriate content](#).

For GCWiki help contact: [webteam](#) RUSSETT [REDACTED]. [Support page](#)

# PHANTOM PARROT

From GCWiki

Jump to: [navigation](#), [search](#)

PHANTOM PARROT is a [GTAC](#) tool that allows the querying of mobile phone data, acquired from police forces under ITT Op WILDWAY, an [AGAP Target Discovery](#) project to acquire and analyse the data.

SIGAD: UKC1164

PDDG: 7C

Enter these into Ariel TDS when reporting!

## Contents

- [1 Background](#)
- [2 Source](#)
- [3 Legalities](#)
- [4 Getting an account](#)
- [5 Reporting](#)
- [6 The port reports](#)
- [7 The tool](#)
- [8 Value to areas other than ITT](#)
- [9 Reference](#)
- [10 Great examples of where PP data has added value](#)

## Background

This mobile phone data is downloaded from people stopped at UK ports (i.e. sea, air and rail). It includes anything stored on a target's phone, although only phonebooks, sms and call events are currently databased and queryable through PP. The data is received via CD on an ad hoc basis (about once a month for London terminals, less for [NPAC](#) so far).

## Source

The data is largely comprised of people stopped by police forces at another service's request. Mainly BSS.

Police also stop people arbitrarily or based on profiling, however unless substantial traces are found against that person, mobile phone downloads are deleted.

Approximately half of all the data (by numbers stopped) is obtained from Metropolitan Police Counter-Terrorist Command (Met CTC / SO15) National Ports Office (NPO), who have responsibility for London City Airport, St Pancras (Eurostar) and Heathrow, where they are based. The rest of the data is collated by National Ports Analysis Centre (NPAC), based at Merseyside Police HQ. Not all ports collect the data during ports stops at present, notably Stanstead and Gatwick, although work is being undertaken to convince them of its value.

## Legalities

The data is legally volunteered under s.7 and s.8 of TACT (Terrorism Act 2000), although the person will not be directly told their phone is downloaded. For this reason normal SIGINT rules about content do not apply, however all queries/use of the data should be proportionate. Think RANNOCH MOOR (i.e. don't include names and addresses in reports just because you can).

## Getting an account

At present PHANTOM PARROT has a maximum of 30 users, however, a new version is due to be released by mid-May, pending the new experiment environment, which will enable it to support over 100. Currently the 30 are all taken, but if you have a legitimate requirement (currently limited to CT) then please contact [REDACTED] who will do his best to accommodate this, or at worst, place you on waiting list for the new version.

PHANTOM PARROT data is one component of [LUCKY STRIKE](#), a collateral 'weak identifier' trace database, currently in development. PP is anticipated to be subsumed into LS at which time the standalone tool will be decommissioned. It is hoped LS will be an early plug-in for [LOOKING GLASS](#).

## Reporting

So, you've got an account, you've found something of interest, how do you EPR it?! First off, use the rule of thumb [REDACTED] (ITT Chief Reporter) gave us: If it was meant for transmission or had already been transmitted, then treat it as though we intercepted it. If not, then quote it as collateral (in all cases SECRET). So:

Phonebook entries - collateral (SECRET)

SMS or MMS drafts, sent items or received - as though you found it in DISHFIRE (although unlike DISHFIRE you can report UK SMS)

Call logs - As though call records, but remember that all times are local and you may not easily be able to tell what local time was (given most will just have arrived from abroad).

Media (you can't search on this presently but you can ask [REDACTED] if you find a stop of significance)

- collateral (SECRET)

Example: (GCHQ Comment: According to collateral (SECRET), 447717171717 was stored as "Davemob" in the phonebook of Op EXAMPLE target Jim.)

Important to remember:

1. If your analysis of the data has generated some completely new intelligence, be that a selector, content or otherwise, then check with your BSS SFO whether it is already known. Remember, a high proportion of the stops are likely to be BSS requested and that just because they never told you, it doesn't mean they don't know.
2. If it just adds to an existing piece of work (i.e. adds some context to a number in your CRA report) then do as you please, but if you are going to make a lot out of it see point 1.
3. Ensure you manually enter into Ariel TDS:

SIGAD: UKC1164

PDDG: 7C

Getting more reliable updates to the data is dependent on proving its worth. If you have any great examples, please enter them at the bottom of this page.

## **The port reports**

If you find your target in the phonebook of someone who is not a target, or you identify a phonebook which looks like it is of interest but again not a target, you may want to request the port report. The report is the result of the police officers interview of the person and will note other important things like other items of interest in their possession and the officer's read-out on the person. If this sounds like it will be of benefit: 1. Check with your SFO, as BSS will receive a copy of the report for any stop they request. 2. If they can't find a report then contact [REDACTED]. At present there is no better way than to request it than from the police force who stopped them, therefore consider its potential value before requesting it.

## **The tool**

PHANTOM PARROT phonebooks are stored by IMSI and IMEI, although we are encouraging ports to record MSISDN this is not yet standard and therefore not uploaded as part of the process of databasing done by [REDACTED]. Phonebook entries are not currently normalised, although this is part of next update due by end-April. CORINTH and MOONRAKER fuzzy matching provides you scores which should give you an idea of whether numbers in a phonebook have been seen in either. A score of around 0.75 and above should be a good match, but always check it.

## **Value to areas other than ITT**

Since first checking the data against CORINTH, targets of MENA and APT have both been noted amongst the stops. As such, the medium term plan is for analysts in all IPTs to have access, although not yet feasible.

## Reference

Page owned and maintained by [REDACTED] (OPIX-ITT-AGAP-Target Discovery) and [REDACTED] (OPD-GTAC). Most questions should be answerable by us, but we are full-time analysts, so please see if this page can answer them first. In case of emergency (i.e. threat to life) [REDACTED] or his Met GCO team should be able to facilitate you getting a port report quickly.

Last updated 27 May 2009.

## Great examples of where PP data has added value

1.
  - a) EPR ref:
  - b) Type(s) of data used:
  - c) Brief comment:

2.

- a)
- b)
- c)

Retrieved from "[REDACTED]"  
[Category: No Category](#)

### Views

- [Page](#)
- [Discussion](#)
- [Edit](#)
- [History](#)
- [Delete](#)
- [Move](#)
- [Watch](#)
- [Additional Statistics](#)

### Personal tools

TOP SECRET STRAP1 COMINT

The maximum [classification](#) allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to [report inappropriate content](#).

For GCWiki help contact: [webteam](#) RUSSETT [REDACTED]. [Support page](#)

# FININT Tasking

From GCWiki

Jump to: [navigation](#), [search](#)



## Contents

- [1 GCHQ's FINANCIAL DATA](#)
- [2 LUCKY STRIKE and LUCKY ESCAPE](#)
- [3 TRACFIN](#)
- [4 CT ONLY FINANCIAL ENQUIRY](#)
- [5 LINKS](#)

## [\[edit\]](#) GCHQ's FINANCIAL DATA

**A check of GCHQ's and NSA's financial datasets should always be considered, not just when your target is involved in finance or when you discover a bank account or credit card for them.**

**Financial data is 'just another data source' and Financial Intelligence or FININT could provide new leads, selectors and geo-location on any target from a search of their name, address, phone no (mob, landline, business), IMSI, email address, business name, as well as bank account or credit/debit card number.**

- GCHQ retain bulk banking data from financial institutions in the Middle East, Pakistan, Zimbabwe and Kenya, and bulk credit card transaction data.
- Stored on AAS EXPERIMENT and a number of biographical FININT datasets are available to query in [LUCKY STRIKE](#).
- Other FININT datasets that cannot for legal and policy reasons be made available in LUCKY STRIKE will be included in a new Finance/Travel tool in development: [Lucky escape](#) (restricted access).
- Please contact [REDACTED], [REDACTED] or [REDACTED] **GCHQ Travel & Finance Data Senior User** [REDACTED] for further details and/or to request access.

The details required for a FININT check are outlined in the [FININT Tasking template](#), see also

## [\[edit\]](#) LUCKY STRIKE and LUCKY ESCAPE

- [LUCKY STRIKE](#)

CT FININT are working with the Finance/Travel Senior User and OPPEG to make bulk selectors derived from financial datasets available via [LUCKY STRIKE](#) and access permitted to all LUCKY STRIKE users. LUCKY STRIKE is an analyst tool which enables a target identifier to be searched against many collateral datasets, with the aim of enriching the 'seed' selector and providing context and additional information. LUCKY STRIKE currently holds over a billion records across 40+ unique datasets, ranging from GSM subscriber details to FININT data.

- [Lucky escape](#)

LUCKY ESCAPE enables analysts to quickly run unselected TDI's (e.g. MSISDN, email, passport) against a multitude of travel and financial datasets, with a view to answering the simple questions 'has my target travelled anywhere?', 'has my target a bank account, credit card and/or have they made any financial transactions?'. The Senior User is [REDACTED] **GCHQ Travel & Finance Data Senior User** [REDACTED]. The datasets which sit behind LUCKY ESCAPE are linked together by field types. This enables very powerful, and very fast, data fusion.

## [\[edit\]](#) TRACFIN

To request a [TRACFIN](#) check:

- It must be minimum UK/US Eyes
- Contact one of the GCHQ TRACFIN Users in your area, go to [TRACFIN Users](#) for a current list or
- Contact [REDACTED] or [REDACTED].

If you do not have a TRACFIN account and would like a TRACFIN analyst to submit a check on your behalf, the information required is:

- Target (name & nationality)
- Target location (address if known)
- SIGINT selectors
- Financial selectors (account details, credit card numbers, money transfer reference)
- Any additional target information (e.g. aliases, companies controlled)
- Justification (Op name if applicable)
- Legalities: JIC Purpose & Priority, Miranda no, Warrant or STA (if applicable)

[TRACFIN request form](#)

## [\[edit\]](#) CT ONLY FINANCIAL ENQUIRY

- Sensitive source covered by an ECI
- Requests may be submitted for **counter-terrorism purposes only** i.e.
  - The person should be either a member of a terrorist group, a suspected extremist, a facilitator, terrorist fund-raiser or otherwise involved in extremist activity or
  - An associate or relative if no more than one step removed from the target.

- Also, it is possible to search wives, husbands or even children's names if you have reason to believe they may set up accounts in their details.
- Intel can derive from any source but must be minimum UK/US Eyes.
- Complete the [FININT Tasking template](#)
- Submit to [REDACTED] or [REDACTED]
- Results are usually returned in 7-14 working days, if the enquiry is threat to life, a 24 hour turnaround is possible
- Results are issued in a plain text word document and can be reported in EPR's subject to data owners approval

## [\[edit\]](#) LINKS

### NSA PLATINUM PLUS/FOLLOW THE MONEY TEAM SUPPORT:

[REDACTED]

TRACFIN: [REDACTED]

FINANCIAL REFERENCE GUIDES (FINTOOLS): [REDACTED]  
[REDACTED]

TAPERLAY: [REDACTED]  
[REDACTED]

TMM: [REDACTED]

MOON RAKER: [REDACTED]

BROAD OAK: [REDACTED]

FININT TRACKER: [REDACTED]  
(restricted access)

### ADDITIONAL INFORMATION

Update BROADOAK with your Financial Selectors as the FININT Team is working with IPLO to link LUCKY STRIKE searches to BROADOAK. This is still in the discussion stages but be prepared!

Retrieved from [REDACTED]

#### Views

- [Page](#)
- [Discussion](#)
- [Edit](#)
- [History](#)
- [Delete](#)
- [Move](#)
- [Watch](#)

- [Additional Statistics](#)

**Personal tools**

- [REDACTED]
- [My talk](#)
- [My preferences](#)
- [My watchlist](#)
- [My contributions](#)

**Navigation**

- [Main Page](#)
- [Help Pages](#)
- [Wikipedia Mirror](#)
- [Ask Me About...](#)
- [Random page](#)
- [Recent changes](#)
- [Report a Problem](#)
- [Contacts](#)
- [GCWeb](#)

**Search**




**Toolbox**

- [What links here](#)
- [Related changes](#)
- [Upload file](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)

[Powered by MediaWiki](#)

- This page was last modified on 24 April 2012, at 16:05.
- This page has been accessed 1,148 times.
- 

---



---



---



---

- [\\_\\_\\_\\_\\_](#)
- [\\_\\_\\_\\_\\_](#)
- [\\_\\_\\_\\_\\_](#)

TOP SECRET STRAP1 COMINT

The maximum [classification](#) allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to [report](#)