

# APPLIED RESEARCH

## Target Detection Identifiers

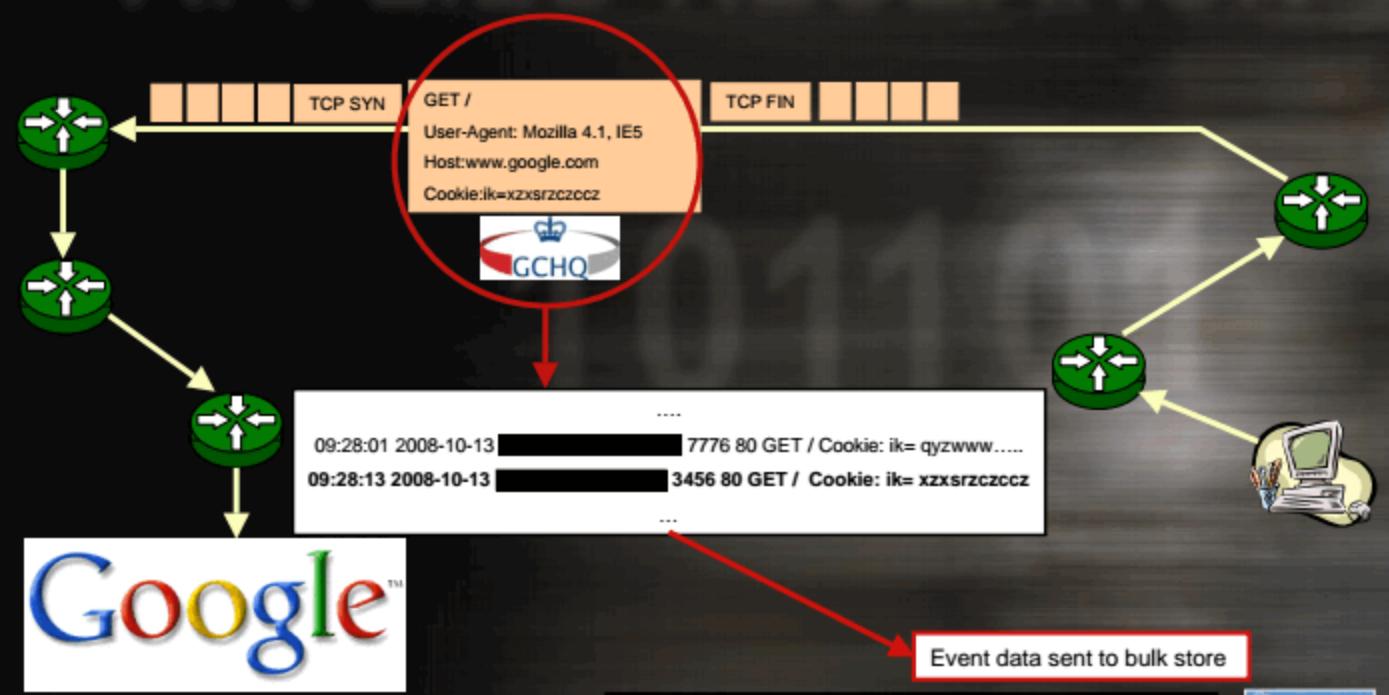
March 2009

© This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to [REDACTED]

Slide 1



# High-Speed Internet Processing



© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

# High-Speed Internet Processing

- Bulk events key to SIGINT success on Internet
- Event types that are valuable for Intelligence change (quickly)
  - 2000 SMTP/POP3
  - 2001 Webmail
  - ...
  - 2007 vBulletin
  - 2008 Social Networks,...,?
- GCHQ's Applied Research are pioneering ways of dealing with this:
  - Presence Events (TDI)
  - Very large scale high speed flat file storage to bulk store TDIs
  - Just enough data marts

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



## IP Packet Information

- Many possible types of information
- Many techniques available
- HTTP Get requests dominate cutting edge techniques
- To get Intelligence value Information must relate to a person or device... a TDI

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ. Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



UK SECRET STRAP2 COMINT ORCON

TDI ...?



© Crown Copyright

other UK information legislation. Refer disclosure requests

under

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

Slide 5



UK SECRET STRAP2 COMINT ORCON

UK SECRET STRAP2 COMINT ORCON

TDI ...?



© Crown Copyright

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

Slide 6

UK SECRET STRAP2 COMINT ORCON



TDI

Target

Detection

Identifier

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



TDI

Target

Detection

Identifier

Who

When

Where

(doing) What

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



TDI

Target

Detection

Identifier

Who

When

Where

(doing) What

Fundamental atom of the Internet age.

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



# Target Detection Identifiers

- **DEFINITION**

- TDIs are **definite** indicators of presence, that are **unique** and **persistent** for a user/machine.

- Built on the familiar

- Telephony +44 – international phone code
  - Signalling tells us this phone user is ‘online’

- Target Detection Identifiers

- Started with the Internet, mobile networks too.
  - TDI is a ‘SIGINT standardised code’.
  - Not a standard managed by the ITU/ETSI.
  - Extraction from packets much more complex.

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



## TDI sources



© Crown Copyright. All rights reserved.

Disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

APPLIED  
RESEARCH

# Target Detection Identifiers

- 70 distinct TDI types discovered.
- 2500 TDIs/sec (GET, de-duplicated)
- => 200 Million per day per 10Gbps
- De-dupe rate ???
- Cost – 250 hours per TDI
- Automated discovery prototype

TDI Type	TDI Location	User/Machine
Yahoo-Y-Cookie	Cookie	User
Yahoo-B-Cookie	Cooookie	Machine
Google-IK	Request-URI	User
Paltalk-Nickname	Request-URI	User
MS-MUID-Cookie	Cookie	Machine
Google-SID-Cookie	Cookie	Machine
Maktoob-MEUser-Cookie	Cookie	User
Orkut-PREFID-Cookie	Cookie	User
Cloob-Username	Cookie	User

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000. Contains intellectual property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



Search GCHQ

**SECRET**

Domain	Context	Technology Selector	Example value	Bearer count	Observation count	Mean user transmission frequency	Cross-/16 percentage
facebook	Cookie	<a href="#">datr=</a>	[REDACTED]	8	671	12.98	3.51
facebook	Cookie	<a href="#">c_user=</a>	[REDACTED]	8	651	12.09	3.51
facebook	Cookie	<a href="#">_utmz=</a>	[REDACTED]	7	609	12.14	4.25
facebook	Cookie	<a href="#">_utmz=</a>	[REDACTED]	7	609	12.44	3.56
facebook	Cookie	<a href="#">_utma=</a>	[REDACTED]	7	601	12.37	3.74
facebook	Cookie	<a href="#">_h_user=</a>	[REDACTED]	7	601	10.38	4.97
facebook	Cookie	<a href="#">_ocam=</a>	[REDACTED]	6	364	10.67	0.24
reuters	Cookie	<a href="#">lv=</a>	[REDACTED]	6	326	16.63	9.18
facebook	Cookie	<a href="#">next_path=</a>	[REDACTED]	6	323	10.81	3.24
live	Cookie	<a href="#">MUID=</a>	[REDACTED]	7	321	21.59	0.45
reuters	Cookie	<a href="#">id=</a>	[REDACTED]	6	312	16.83	5.81
google	URI	<a href="#">q=</a>	[REDACTED]	7	311	16.02	0.39
reuters	Cookie	<a href="#">ss=</a>	[REDACTED]	6	309	16.33	2.76
yahoo	Cookie	<a href="#">B=</a>	[REDACTED]	7	307	10.60	7.79
yahoo	Cookie	<a href="#">d=</a>	[REDACTED]	6	306	24.90	1.96
youporn	Cookie	<a href="#">side=</a>	[REDACTED]	5	282	24.23	1.65
youporn	Cookie	<a href="#">_utma=</a>	[REDACTED]	5	281	22.92	4.60
reuters	Cookie	<a href="#">anonid=</a>	[REDACTED]	6	279	16.22	0.46
youporn	Cookie	<a href="#">_ocam=</a>	[REDACTED]	5	277	24.40	1.69
yahoo	URI	<a href="#">p=</a>	[REDACTED]	7	277	31.18	2.06
bobo	Cookie	<a href="#">bdaysession=</a>	[REDACTED]	7	275	27.19	7.31
google	Cookie	<a href="#">LM=</a>	[REDACTED]	7	272	16.85	3.73
google	Cookie	<a href="#">ID=</a>	[REDACTED]	7	271	16.80	6.57
google	Cookie	<a href="#">TM=</a>	[REDACTED]	7	270	27.18	2.21
bobo	Cookie	<a href="#">Username=</a>	[REDACTED]	7	268	27.67	2.24
bobo	Cookie	<a href="#">Email=</a>	[REDACTED]	7	268	39.35	3.00
yahoo	Cookie	<a href="#">l_se=</a>	[REDACTED]	4	264	14.24	3.82
google	Cookie	<a href="#">S=</a>	[REDACTED]	6	253	66.03	2.54
yahoo	Cookie	<a href="#">ip=</a>	[REDACTED]	3	251	17.07	1.01
yieldmanager	Cookie	<a href="#">uid=</a>	[REDACTED]	7	242	17.85	0.48
reuters	Cookie	<a href="#">RaptTracker=</a>	[REDACTED]	6	242	17.85	7.19
yahoo	Referer	<a href="#">p=</a>	[REDACTED]	4	242	11.09	2.70
gchq	Cookie	<a href="#">_ga=</a>	[REDACTED]	6	242	11.09	2.70

## TDI Applications

- Bulk store of all TDIs seen in last 6 months [MUTANT BROTH]
- Bulk store TDI correlations (6 months) [AUTO ASSOC]
- Bulk store TDI <-> website correlations (6 months) [KARMA POLICE]
- Bulk store TDI vBulletin activity [INFINITE MONKEYS]
- Bulk store TDI Social Networking Site activity [SOCIAL ANIMAL]
- Bulk store web search requests [MEMORY HOLE]
- Bulk store Google Earth requests [MARBLED GECKO]
- Bulk store of Host Referer references [HRMARI]

© Crown Copyright. All rights reserved. This document contains neither recommendations nor conclusions of the Government. It is the copyright holder's intention that it should not be distributed outside the recipient organisation without GCHQ permission. It may contain sensitive information and may be subject to exemption under other UK information legislation. Refer disclosure requests to Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



**SECRET**

**HUTANT BROTH**

Identifier Search IP Address Search Password Search

Welcome

Logged In as [REDACTED] all queries logged for audit.

Database currently contains Identifiers from the period Tue Dec 25 16:26:40 2007 to Fri Jun 20 22:13:19 2008 (18.41 billion rows of as 07-JUN-08).

**Warning: data for period(s):**

- Fri Jun 20 22:13:21 2008 - Tue Jun 24 09:33:20 2008

is loaded, but currently unavailable for query due to index building. The rest of the database can be queried as usual during the rebuild.

**Search for Identifiers**

- If allow wildcards is ticked, % and \_ are multi-character (bob%) and single-character (b\_b@hotmail.co) wildcards.
- Queries are always case-sensitive (bob@hotmail.com ≠ BOB@hotmail.com ≠ 808@HOTMAIL.COM). There is an option to automatically convert to lowercase.
- For bulk queries, paste in a list of identifiers separated by newlines (one per line).
- You can enter a minimum/maximum date for the search: default is to search all available selectors

MIRANDA 20135  
 JIC 1  
 Purpose NS  
 Reason demo

Allow wildcards  Convert to lowercase before searching

**Matching Identifiers**

The following identifiers have been found in the HUTANT BROTH database.  
Select those that match your target(s) to generate a summary of target activity.

TDI type	TDI value
<input type="checkbox"/> Chat-MS-Messenger	[REDACTED] @hotmail.fr

**SECRET**

MUTANT BROTH

Identifier Search IP Address Search Password Search

Welcome

Logged in as [REDACTED] all queries logged for audit.

Database currently contains identifiers from the period Tue Dec 25 16:26:40 2007 to Fri Jun 20 22:13:19 2008 (18.41 billion rows of as 07-JUN-08).

**Warning: data for period(s):**

- Fri Jun 20 22:13:19 2008 (18.41 billion rows of as 07-JUN-08). **rebuild.**

**Search for Ident**

If allow wildcards is selected, one can search for multiple identifiers (e.g. \*bob\*) and single identifiers (e.g. bob@hotmail.com).

Queries are always case-sensitive (bob@hotmail.com ≠ BOB@hotmail.com ≠ bob@outlook.com). There is an option to automatically convert to lowercase.

For bulk queries, paste in a list of identifiers separated by newlines (one per line).

You can enter a minimum/maximum date for the search: default is to search all available selectors

MIRANDA 20135  
 JIC 1  
 Purpose NS  
 Reason demo

Allow wildcards  Convert to lowercase before searching

**Matching Identifiers**

The following identifiers have been found in the MUTANT BROTH database.  
Select those that match your target(s) to generate a summary of target activity.

TDI type	TDI value
<input type="checkbox"/> Chat-MS-Messenger	[REDACTED] @hotmail.fr

**SECRET**

Date	Time	Source IP	HHFP	Source IP Geo	Identifier Type	Identifier Value	Passw
17/06/2008	17:08:44	[REDACTED]	[REDACTED]	6de32bb0 41.02;28.96;ISTANBUL;TR;5MMM	Hi5-Email-Cookie	[REDACTED]@hotmail.com	
17/06/2008	16:55:21	[REDACTED]	[REDACTED]	6de32bb0 41.02;28.96;ISTANBUL;TR;5MMM	Hi5-Email-Cookie	[REDACTED]@hotmail.com	
17/06/2008	16:55:16	[REDACTED]	[REDACTED]	6de32bb0 41.9022;-87.6726;CHICAGO;US;5MML	Hi5-Email-Cookie	[REDACTED]@hotmail.com	
17/06/2008	16:54:47	[REDACTED]	[REDACTED]	6de32bb0 41.9022;-87.6726;CHICAGO;US;5MML	Hi5-Email-Cookie	[REDACTED]@hotmail.com	
17/06/2008	16:52:13	[REDACTED]	[REDACTED]	6de32bb0 39.94;32.86;ANKARA;TR;5MMM	Hi5-Email-Cookie	[REDACTED]@hotmail.com	
15/06/2008	19:20:33	[REDACTED]	[REDACTED]	de8bdc48 33.5;36.3;DIMASHQ;SY;5MLV	Hi5-Email-Cookie	[REDACTED]@hotmail.com	

**WHEN**

**WHERE**

**WHO**

**WHAT**

## Other Bulk Event Applications

- Most events that can be associated back to TDIs:
- File Transfer Signature (eg proof of life videos)
- Detection by Internet profile – eg 'Dead Letter Drop'.
- Yahoo webcam images
- Airline reservation confirmation emails

© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

