

SECRET STRAP1 COMINT

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

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

Event (SIGINT)

From GCWiki

(Redirected from [Event \(communications\)](#))

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

An **Event** within a [SIGINT](#) context refers to a [phenomenon](#), something observable at a given time. Typically, an event results from a direct observation of an electronic communication of some form but it could also result from other sources.

Events contain only [metadata](#) and do not contain message content. Sometimes there are grey areas between events and content. For example the subject of an e-mail is generally transmitted in the header portion of the message that contains the Events metadata. However the subject can be considered Content because it reveals information about the purpose of the message (as is the current interpretation).

There are generally fewer legal restrictions about the collection and processing of events than content items. This is one enabler of events bulk collection and retention, which is not generally possible with content.

Contents

- [1 Event Granularity](#)
- [2 Types of Event](#)
 - [2.1 Comms Event](#)
 - [2.2 Presence Event](#)
 - [2.3 Social Event](#)
 - [2.4 Geo reference Event](#)
- [3 Derived Events](#)
 - [3.1 Convergence](#)
 - [3.2 Correllation](#)
- [4 Events Databases](#)
- [5 Interface Control Documents \(ICDs\)](#)
 - [5.1 INTERSTELLAR DUST \(IDUST\)](#)
 - [5.2 Actor Action \(AA\)](#)
- [6 See Also](#)

[\[edit\]](#) Event Granularity

More than one definition of an event is in use. In HAUSTORIUM (Now Decommissioned and replaced with [SOCIAL ANTHROPOID](#)) an event normally has the granularity of a single message. The observation of an e-mail constitutes a single event, even though the e-mail may be addressed to many people. Other projects may define an event in a slightly different way. For example several distinct

communications involved in sending a single message may each form a separate event.

On occasion single events can end up being split into multiple events because of the nature of the intercept mechanism. For example an e-mail may be split into individual messages by [Mail Transport Agents](#) when delivering a single message to multiple destinations. This can result in the appearance of multiple events depending on the point at which the event was intercepted.

Conversely, an event can be the summarisation of many individual transactions, taking place over a long period of time. For example, instant messaging text chat events in HAUSTORIUM are actually the summarisation of a series of separate messages, each of indicates people joining and leaving the chat, inviting others and accepting invitations etc. The final event that is presented to the analyst shows only the group list of people involved, in order to avoid swamping the analyst in huge numbers of separate trivial rows of data.

[\[edit\]](#) Types of Event

Example Event types from Mobile traffic

Events have traditionally been categorised according to the technology involved - [Telephony](#), [C2C](#) and [Geo](#). GCHQ is currently developing a more activity-centric (and technology agnostic) view based on types such as:

- Communications (Comms) Events
- Presence Events
- Geo reference Events

The [Mobile Applications Project](#) have drawn up a diagram showing the relationships between some example event types: [RightArrow.jpg](#)

[\[edit\]](#) Comms Event

A Communications or Comms Event occurs when one party communicates with another. Comms Event types include:

- Telephone calls, both landline and mobile
- C2C telephony: VoIP and SIP
- Correspondence: sending and reading emails, including webmail

[\[edit\]](#) Presence Event

Presence Events are defined by the **INTERSTELLAR DUST ICD** - see [IDUST \(PPF App\)](#). This includes:

- Presence TDIs - real world events where there is an active user (e.g. logging into a website, requesting a web page)
- Google Maps and Earth events - where the active user has requested a map tile
- HTTP Get and Post - where the user has requested a web page
- Web search events - where the active user has searched for something (e.g. in google)
- Telephony presence (i.e. location updates, or other location information about the active user contained in the signalling)

[\[edit\]](#) Social Event

Social events are currently being defined by the new **Actor-Action ICD** - see [PPF APPS Actor Action Event](#). Still in draft, this is to cover events where the user is interacting with a subject (e.g. another communicant or object). There is no need for an active user in these events. Examples are various, but could include:

- Webmail
- Chat
- [Mobile apps](#) will form new actions within the model e.g. User X sends MMS to User Y

[\[edit\]](#) **Geo reference Event**

Geo Reference Events provide information about the global communications network.

They will be geo-labelled using [SAMREF](#) or [GEOFUSION](#) as appropriate using the standard geo label (as agreed by the [Geo](#) Team).

[\[edit\]](#) **Derived Events**

Once some events have been collected, various analytics can be applied to derive useful relationships between them:

[\[edit\]](#) **Convergence**

[ArrowRight.png](#) *See main article — [Converged Events](#)*

Converged Events is the association of events from different SIGINT universes, such as Telephony and C2C, for a given target.

[\[edit\]](#) **Correllation**

TDIs from collected events can be correlated together to form correlation records (e.g. in HARD ASSOC between IMSI-TDI)

[\[edit\]](#) **Events Databases**

GCHQ Events databases

[Eye Icon.png](#) *See also — [Query focused dataset](#)*

- [SOCIAL ANTHROPOID](#) - C2C Comms and Social events QFD, has replaced HAUSTORIUM.
- [SALAMANCA](#) - Telephony events. Due to be subsumed into SOCIAL ANTHROPOID.
- [NGE Input Buffer](#) - C2C events warehouse. User access is not usually direct, but via one of the [QFDs](#).

[NSA](#) Events databases and systems

- [ASSOCIATION](#) - [GSM](#) events
- [BANYAN](#) - Telephony events
- [MAINWAY](#) - [contact chaining](#)

The NSA systems and databases above derive their metadata from the [FASCIA](#) data repository

- [CULTWEAVE II](#) - [VOICESAIL](#) events

Old Events databases

- [TEEDALE](#) was superseded by [PILBEAM](#) which in turn was superseded by HAUSTORIUM
- HAUSTORIUM - C2C events

[\[edit\]](#) Interface Control Documents (ICDs)

Events are forwarded in a format specified in an ICD. Traditionally each database, e.g. SALAMANCA or HAUSTORIUM, has had its own ICD. With the arrival of QFDs and the requirement for Convergence it is becoming necessary for ICDs to focus on the Event type rather than any specific database.

The most important new ICDs in use are:

- [INTERSTELLAR DUST](#) (IDUST)
- [Actor Action](#) (AA)

[\[edit\]](#) INTERSTELLAR DUST (IDUST)


 See main article — [INTERSTELLAR DUST](#)

IDUST was the first ICD capable of covering new GTDIs (Presence Events}. It is a Single-Line Record (SLR) format.

Each Event type is specified individually in the ICD. They include:

- Presence Events (for MUTANT BROTH, AUTOASSOC)
- Google Maps/Earth (for MARBLED GECKO)
- HTTP GET & POST (for KARMA POLICE)
- HTTP Host Referer (for HR MAP)
- Web Search (for MEMORY HOLE)
- VBulletin (for INFINITE MONKEYS)
- Social Networks (for SOCIAL ANIMAL)
- Auto TDI (for AUTO TDI)
- HTTP Host URI (for SAMUEL PEPYS)
- FTP (for SAMUEL PEPYS)

[\[edit\]](#) Actor Action (AA)

 See main article — [PPF APPS Actor Action Event](#)

AA is the newest ICD. It provides a generic schema allowing for different types of Event. It is replacing the old CorrespondenceData, PresenceData, IMData and IMdataOffbox formats while new event types are also being developed, for example for Mobile Apps. Some IDUST Events are also likely to migrate across to AA, while others may remain in IDUST format.

AA is initially intended to cover Presence and Communication (Social) Events only:

- Presence (GTDI) (for HARD ASSOC, evolved MUTANT BROTH)
- Communication (for SOCIAL ANTHROPOID)

Protocols and Apps currently adopting AA format include:

- email: SMTP, POP3, IMAP, Webmail (inc Mobile),
- messaging: IM (ICQ), MMS
- VoIP: SIP, H323
- GTP: Gn, Gp (GRX)
- General Apps: Google Mobile Maps, BlackBerry

[\[edit\]](#) See Also

- [Operational Legalities Policy FAQ for Events](#)
- [Where is My Event](#) for more info on why you may or may not see events data on your target.
- [Next Generation Events](#) (NGE) project
- [TDB Events Product Centre](#)