



Investigator: Why is it different?

Investigator was designed by investigators for use by their fellow investigators. From the outset the goal was to produce an easy to use, very secure and highly responsive investigation management system.

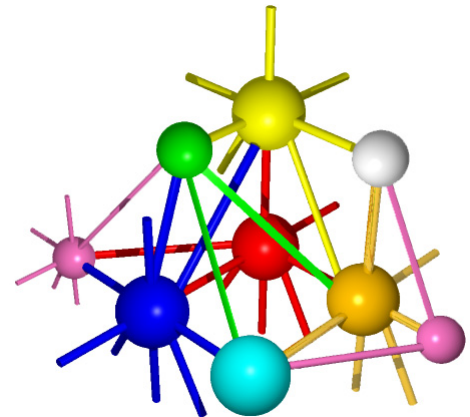
Here are some reasons why we believe Investigator is different from other investigation management offerings.

Architecture

- conceived and built as single application that seamlessly manages all investigative and intelligence information
- every real world entity, relationship and attribute has a source document that provides a reference for its existence
- single entry for all data, single search for all data

Technology

- the use of a tightly integrated object oriented development environment and object database gives considerable advantages in application development speed, flexibility and capability over conventional applications
- no changes required to application or database to move from single user on a notebook to thousands of users on an international network
- no third party products are required to deploy the application on any scale (Microsoft Office is optional for deployment on workstations)



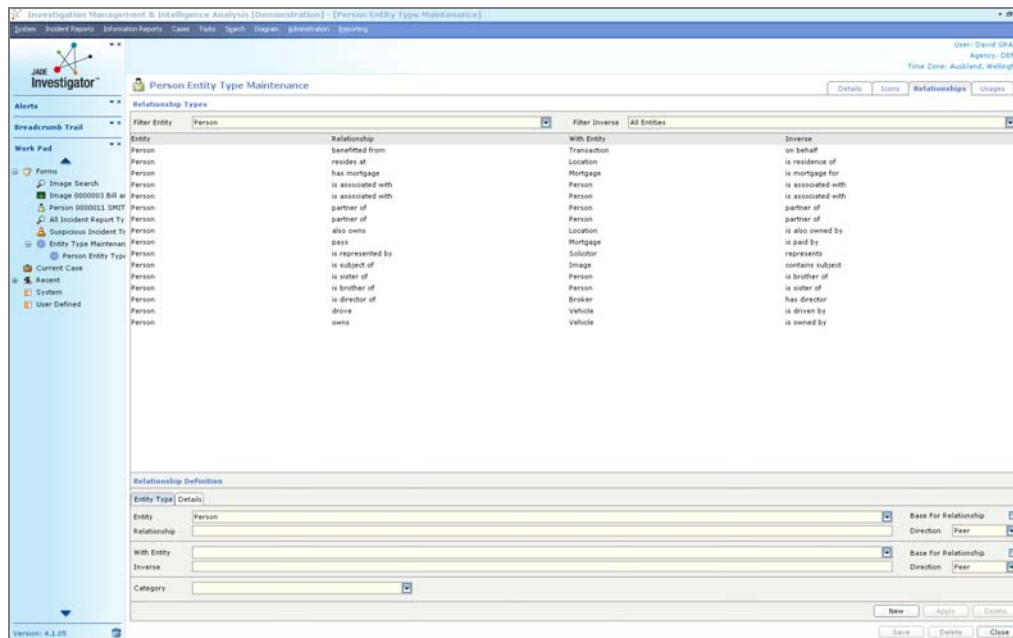
Applicability

- conceived as a generic investigative and intelligence system capable of being configured to suit any agency
- interface is translatable into any Unicode language in days
- stores and searches on any Unicode text, even mixed in the same document

- incorporates the features of narrowly focussed, single user or work group sized, specialised applications in a single enterprise application

Configurable

- user defined system entity types e.g. cases, case notes, information reports, incident reports, tasks each type having their own attributes, behaviour and security
- user defined tangible entity types e.g. person, contact number, document with new types inheriting from existing native entity types or being created independently



- user defined relationships between system and tangible entities
- user defined attributes for any entity that are capable of recording and searching for any structured information about that entity, attribute types include calculated, code table, text, numeric, masked text, date, date/time, user, user collection, warning
- user defined populated code tables that can have different contents ordering behaviour depending on context
- user defined data entry Templates for system entity types
- user defined thesaurus
- user defined layout to load any comma or tab delimited file and automatically create entities, attributes and relationships

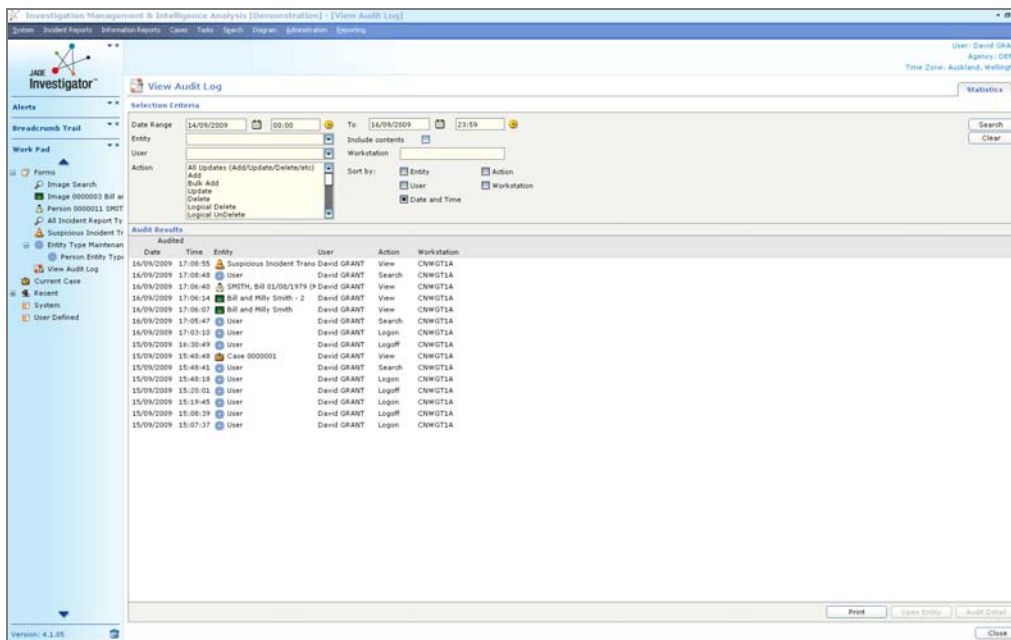
Server security

- the administrator only requires access to the server and does not have or require any access to the data to maintain the application

- there are no third party tools to access or change the data, the only means to access the data is through the application
- Instant application of security
- any change to access to functionality i.e. creating a case, is implemented instantly across the application, there is no need for users to log off and log on again to update settings
- any change to access to data i.e. accessing a case is implemented instantly across the application, there is no need for users to log off and log on again to update settings, if a user has the case open, the case will be closed

Auditing

- all access to the application by every user is audited in a permanent, un-editable record
- every user action from log on to log off is audited including search criteria and versioning of every change



Controlled access to functionality

- access to functionality is controlled by user defined Roles that can be allocated any combination of permissions
- permissions are allocated by entity type and function
- permissions do not have any dependencies or hierarchies, having delete
- permission does not require create or view permission

Controlled access to data

- access to information and incident report data and associated entities is controlled on each individual report
- access to case data and associated entities can be controlled independently at each individual case note ie access to the case does not imply access to all case information
- default access can be allocated to any individual or collection of users

The screenshot displays the 'Case Management Maintenance' interface. At the top, it shows 'Details For Case Management (Number: 0000001)'. Below this, the 'Case Officer' is set to 'GRANT, David (DG)'. The 'Security Access' section is divided into 'Available' and 'Selected (🔴 = View Only)'. The 'Available' list includes 'Bank Officers', 'Investigators Management', and 'Individual Users'. The 'Selected' list includes 'Investigators' with sub-items: 'Can change Case', 'Can maintain Threads', 'Can update Limited Release', 'Case Notes', 'Information Reports', 'Incident Reports', 'Members', and 'Individual Users' (with 'GRANT, David (DG)' listed below it). At the bottom, the case details are shown: Title: 'Investigation of three suspicious transactions - ANDREWS/SMITH/SMITH' and Description: 'Within the past 15 months there have been three suspicious incident transactions that may be connected. The first, in May 2008, involves a property at 31 Green Road, Newtown. This property is referenced in the other two suspicious transactions in January 2009, and August 2009. In all three cases, large amounts of cash were deposited - \$102,000, \$100,000, and \$76,000 respectively. The first transaction involves Peter Andrews. There appears to be no obvious connection between Andrews and the other two transactions. This needs to be investigated.'

Embedded files

- all externally generated files such as relevant Word documents are loaded and embedded in the database, subject to auditing and security

Allows controlled data sharing

- multiple organisations or departments can use the same database, administer their own users and choose how their data is shared, if at all

Accurate and flexible recording and searching for date and time information

- all date and time information can be recorded against the original time zone and is displayed to the user in their own local time, enabling correct chronological ordering and searching across multiple time zones
- all dates and times can be exact (4/7/2007, 14:45:43), unbroken range (4/7/2007 to 7/7/2007, 14:45:43 to 15:23:16), broken range (all Saturdays in April 2007, either 6:00 or 09:00 or 13:00) or Unknown allowing for maximum flexibility in recording date and time information

The screenshot shows a 'Security Access' window with a list of roles on the left: Bank Officers, Investigators, Management, and Individual Users (with a plus icon). A 'Happened' dialog box is open, displaying a calendar for August 2009. The date 12/08/2009 is selected. Below the calendar are 'Clear', 'Unknown', and 'Ok' buttons. At the bottom of the main window, there are fields for 'When Reported' (12/08/2009, 14:38) and 'When Happened' (12/08/2009, 14:15), along with 'Created' (12/08/2009 14:41 by PETERS, John (JP)) and 'Last Updated' (08/09/2009 11:54 by JONES, Mike (MJ)) information.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Exploiting Information

- Information and Incident Reports and case notes from other cases can be included in a case where that information is relevant to the case, these are introduced using a case note that acts as the source document for the introduced information.
- Any information and incident report and case note shows which cases it is contained in

Searching

- all searches are across all data the user has access to irrespective of context, origin or source
- full text searching across all data including embedded Word, PDF, Excel and PowerPoint, text and HTML files, including wildcards, boolean and precedence operators
- attribute searching for any entity type using multiple attribute criteria, boolean and precedence operators
- thesaurus search using a user defined thesaurus that allows for searching by broader, narrower terms, synonyms and user defined related terms
- define searches that run against newly added or edited information in near real time (< 10 sec) with no polling interval using any of the above search types with automated notification to the user
- search for directly related entities either by two specific entities or by entity types
- search for direct or indirect relationships between multiple entities, filtered by entity type or specific entity directly from the database with no data stripping
- search for repeating instances of related entities (phone calls, email, sms, transactions patterns) across the entire database irrespective of data volume
- display aggregated text related text for any source documents related to any entity
- search for all source documents that have multiple entities in common



Productivity

- simple to use – consistent interface and functionality
- threading – allows traceability of various lines of enquiry in a case
- workpad – a user configurable clipboard to store entities for future use
- breadcrumb trail – a means of recording and retracing the navigation through a series of entities
- watches – immediate notification to user of the view or change to any nominated entity either covertly or overtly
- fully integrated diagramming – diagrams can be drawn in real time from the database from any entity showing all relationships irrespective of context, origin or source, diagram a case or source document or the result of a related entity search

Images

- images are entities, allowing them to be related to many other entities ie relate multiple persons in a surveillance photo to the photo and therefore indirectly to each other, search for photos with person A and Person B in them etc
- unlimited images may be related to any entity, with one being the identification image
- single click to display all images related to any entity
- allow images to be annotated with text or specific entities with single click navigation to the entity
- chain together an unlimited number of images of increasing level of detail allowing infinite drilldown and navigation from any area of interest in an image i.e. drilldown from a photo of a car to a photo of the front door to a photo of the door handle to a photo of a fingerprint on the door handle to a specific area of interest on the fingerprint

