Netherlands Forensic Institute
Ministry of Security and Justice

Knowledge and Expertise Centre for Intelligent Data Analysis
part of the **Netherlands Forensic Institute**

Sharing intelligence
Kecida

Sharing intelligence

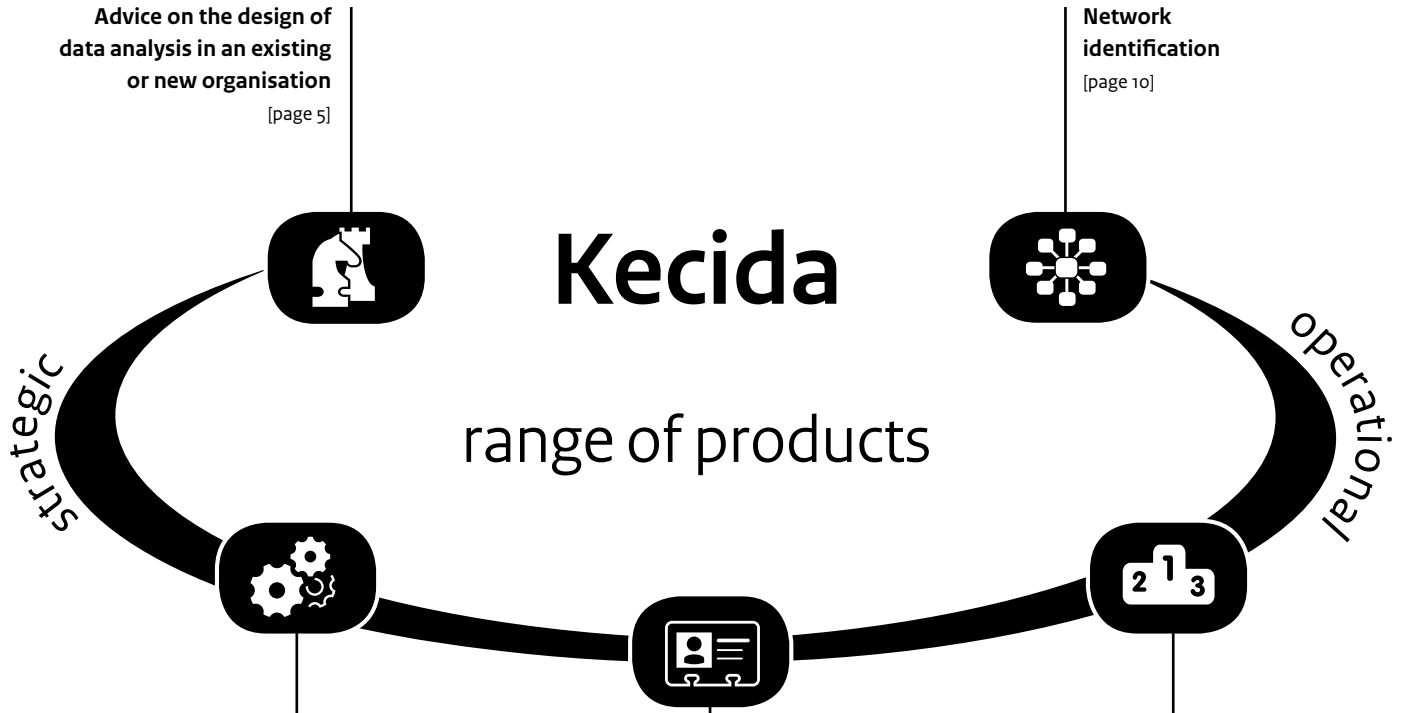
Kecida

Mission

On the instructions of organisations in the Public Order and Security Sector, Kecida provides high-quality services and products in the area of intelligent data analysis using state-of-the-art science and technology.

Kecida...

- has many years of experience at the interface of intelligence and forensics
- provides a comprehensive set of proven state-of-the-art techniques in the Public Order and Security Sector
- provides solutions tailored to each problem
- is part of the NFI and consequently a very reliable, objective and independent government organisation and is also part of the Public Order and Security Sector
- shares the knowledge and expertise it has gained and co-operates intensively with other knowledge institutes such as universities, but also with companies


Advice on the design of data analysis in an existing or new organisation
[page 5]
Network identification
[page 10]
Kecida
range of products
strategic
operational
Tests of existing and development of new methods and techniques for data analysis
[page 6]
Profiles/indicators on the basis of intelligent data analysis enabling the client itself to find deviations
[page 7]
Ranked lists of concrete deviations on the basis of intelligent data analysis
[page 9]

Advice on the design of data analysis in an existing or new organisation

Client request:
What is the best design for our organisation / our process / our systems in the area of data analysis in order to perform our tasks to the best of our ability?

Example:
- Which systems do we need to be better able to combat real estate fraud?
- How can we design our data analysis processes better and what do we need for this?

Proposal:
Kecida provides advice on and assistance in matters concerning data analysis design.

Example:
- Design of data analysis environment (required systems, type of employees)
- Design of data analysis processes
- Selection of suitable data sources

The results will be provided in the form of a report, a management presentation and/or knowledge transfer sessions.

*Examples**

The government had given the organisations that had to do with border control – such as the border police, the immigration service, and customs – the order to develop one virtual environment, making it possible to link data from the different organisations in a smart manner and to perform intelligent data analysis on this basis. Kecida provided strategic advice on the virtual organisation to be developed: which links were necessary between which systems and which organisations had to be involved? Before all this could actually be implemented, Kecida performed tests to establish that the plan did not only work on paper, but also worked in practice. For this purpose, all data were sent to the Kecida lab, after which these data were linked and the required analyses were performed. The plan was adjusted on the basis of the results and subsequently implemented.

An organisation wanted to change its information management and it wanted to change it in such a way that it would be possible to make analyses in the future. They wanted to go from four information systems to one central information system, and they wanted the data analysts to provide specific reports and overviews. Kecida made recommendations on the system requirements, so that the system would have the features and structure to meet the wishes of the organisation in the area of analysis.

A financial investigation service wanted to identify networks of substantial financial fraud at a large organisation that operated internationally, but it did not have the suitable software. Kecida developed a method enabling the data analysts to identify any deviating and/or specific patterns in large quantities of transactions. By means of this method, the investigation service was able to search for specific fraud, for instance real estate fraud; quick resale of premises at considerable price increases. The investigation service was, however, also able to search for deviations which might reveal unusual structures/transaction patterns on the basis of which the investigators were able to investigate what they implied.

* *The examples in this brochure are fictitious and only intended as an illustration of the different applications of the products.*

Tests of existing and development of new methods and techniques for data analysis

Client request:
How can we obtain more information from our existing data efficiently and effectively?

Example:
- How can we improve our samples of companies to be audited?
- How can we keep our profiles up to date?
- How can we include information from the Internet in our investigations?

Proposal:
Kecida tests existing methods and techniques or provides methods and techniques tailored to client needs in order to obtain more and better results from the client's own data analysis environment.

Example:
- Method and technique for improved sampling
- Method and technique for author recognition
- Method and technique for code recognition

The results will be provided in the form of a method, technique or report.

Examples

The data analysts of a large organisation had difficulty analysing the data from the different data files because the data had been polluted. The management intended to purchase data cleaning software for this purpose, but it had no idea which software to buy and called in the help of Kecida. Kecida tested several existing software packages on applicability for its client and gave advice on the purchase of a suitable package.

A financial investigation service suspected a large mail order firm of financial fraud. During a search, it seized 60 PCs and a number of mail servers and it made copies of the hard disks. They wanted to analyse the enormous amount of data seized in a smart manner. In cooperation with the investigation service, Kecida provided 'customised search words'. Using these words the investigators searched and actually found indications of financial fraud. Kecida subsequently updated the search words periodically, so that they could also be used during other investigations.

An organisation had a large number of files of cases relating to serious criminals covering a long period of time. As it concerned hundreds of thousands of pages, it was difficult for the analysts to investigate possible interconnections among the different cases and persons, possible networks, and still unknown facilitators within those cases. Together with the analysts and the investigators, Kecida examined what would be the best way to retrieve the right information and to perform the aforementioned investigations. These consultations resulted in Kecida's development of a tool for the analysts and investigators to answer the required questions easily.

An intelligence service wanted to have radicalising religious people in its sights in time and it therefore closely monitored specific internet forums. At the request of this service, Kecida developed a risk profile with indicators enabling this service to identify suspicious posts quickly in the future and it processed these indicators in a software tool, thus simplifying the work of the investigators.

Profiles/indicators on the basis of intelligent data analysis enabling the client itself to find deviations

Client request:
How can we more effectively recognise suspicious elements better in the mass of persons, goods, documents or transactions?

Example:
- How can we recognise illegal goods in consignment notes or bills of lading?
- How can we recognise fraudulent invoices in financial records?
- How can we recognise suspicious transaction patterns in large financial records?
- How can we recognise radicalising youth in a specific population group?
- How can we recognise sex tourists upon arrival at an airport?

Proposal:
Kecida provides insight into specific features which enable the client to find deviations in the mass of persons, goods, documents or transactions itself.

Example:
- A list of typical features of suspicious persons, groups or organisations
- A list of typical features of suspicious objects or goods
- A list of typical features of suspicious documents, transactions or information flows

The results will be provided in the form of a report (textual and/or visual).

Examples

The border police at an international airport was interested in which of the tens of thousands of passengers that arrived at the airport each day were likely to smuggle drugs or other illegal substances or might be potential terrorists. At the request of the border police, Kecida developed risk profiles with indicators making it possible for the police to identify suspicious persons more quickly and more efficiently in the future.

The police seized a man's PC that contained child pornography. They wanted to know which role the man was playing in a – no doubt – larger network of child pornography: who the possible downloaders and/or distributors or even producers of child pornography in this network were. Kecida analysed all data, such as e-mails, chat traffic and photos, in its own lab and concluded that the man was a producer of child pornography. In addition, Kecida identified the man's network and subsequently made ranked lists of possible downloaders, potential abusers, et cetera, in that network on the basis of automatic language analyses of the chats and the e-mails. This resulted in the names of several new suspects in respect of whom the police could conduct further investigations.

Each Friday, a man arrived at the airport from Bulgaria with two girls. The border police suspected human trafficking, with the girls disappearing into prostitution. This could have resulted in a criminal investigation into this man, with the man being convicted or not. Instead of this immediate and individual-oriented approach, Kecida looked for the whole story and identified a network of human trafficking by analysing the data files of the immigration service, the border police, and the Chamber of Commerce together. This provided insight into the modus operandi and the different roles of the various people involved. The organisations from the Public Order and Security Sector then had sufficient information to take various actions against the brothel owner (the key figure) as well, from actions under administrative law – by withdrawing licences – to financial economic actions and actions under criminal law. In addition, the insight thus obtained made it possible to take preventive measures as well.

Ranked lists of concrete deviations on the basis of intelligent data analysis

Client request:
Can you make a ranked list for us of suspicious persons/objects/documents et cetera?

Example:
- What invoices in these records are suspicious?
- What transactions in these organisations are suspicious?
- What documents on this server are suspicious?
- What are the high-risk agricultural undertakings in this region?
- Who are the potentially dangerous hackers in this news group?

Proposal:
Kecida will provide a ranked list of deviations within a data set.

Example:
- A list of suspicious persons, groups or organisations
- A list of suspicious objects or goods
- A list of suspicious documents, transactions or information flows

The results will be provided in the form of a report (textual and/or visual), where possible, supplemented with a manual for effective application.

Examples

The national investigation service made a copy of a hard disk of the computer of a man who was being suspected of having connections with a terrorist organisation. They wanted to know with whom this man had been in contact and when, what the different subjects of communication were, what the most relevant messages were, and what his precise role was in the organisation. The data were sent to the Kecida lab and Kecida succeeded in identifying the complete network around the suspect on the basis of data including e-mails and chat messages. This clearly showed that the suspect fulfilled a key role in the terrorist organisation and the national investigation service was able to trace seven other prominent figures in the organisation.

A financial investigation service seized all the accounting records of an office of a large bank because there were indications of embezzlement by the management. The enormous amount of data was immediately sent to the Kecida lab. Kecida sorted the data by relevance and subsequently provided a ranked list with the e-mails containing most indications of financial fraud ranked first. Kecida also provided a ranked list of names of people, with the most conspicuous people ranked first. In addition, Kecida identified a network of transactions with account owners, account numbers, money amounts, et cetera. This network was used by the investigators to search for deviations, such as unusually high amounts of money and conspicuous transaction patterns. If desired, Kecida would also be able to perform this search.

Network identification

Client request:
Is there possibly a network here, and if so, what does it look like?

Example:
- What is the scope of this child pornography network and what suspects are involved in it?
- What is the role of this person in this human-trafficking organisation?
- Does the suspected fraudster operate independently?
- Are these aliases of the same person(s)?

Proposal:
Kecida provides an indication of whether there might be a network and what this network looks like.

Example:
- Information on the scope, players, and interconnections
- Information on the roles or identities of the players
- Information on the locations, addresses, account numbers, amounts, et cetera

The results will be provided in the form of a report (textual and/or visual).

Summary - Kecida...

- is the binding factor for all organisations in the Public Order and Security Sector that engage in activities in the area of intelligent data analysis
- has many years of experience at the interface of intelligence and forensics
- provides a broad range of products and services, from a strategic to an operational level, namely:
  - advice on the design of data analysis in an existing or new organisation
  - tests of existing and development of new methods and techniques for data analysis
  - profiles/indicators on the basis of intelligent data analysis enabling the client itself to find deviations
  - ranked lists of concrete deviations on the basis of intelligent data analysis
  - network identification
- is able to analyse both structured and unstructured data, originating from one or more sources
- provides solutions tailored to each problem
- is part of the NFI and consequently a very reliable, objective and independent government organisation and is also part of the Public Order and Security Sector
- shares the knowledge and expertise it has gained and co-operates intensively with other knowledge institutes such as universities, but also with companies

For all products:

- The data may originate from both a single source and from multiple sources
  > **Kecida is able to link data sources**

- The data may be either structured or unstructured
  > **Kecida is able to extract and filter data**

Information
For more information on Kecida's range of products or on other products of the Netherlands Forensic Institute, please contact:

NFI Front Office
Accountmanagement, Marketing & Sales
E-mail accountmanagement@nfi.minjus.nl
Telephone +31 70 888 66 40

Sharing intelligence
Kecida

Knowledge and Expertise Centre for Intelligent Data Analysis
part of the **Netherlands Forensic Institute**

Netherlands Forensic Institute
Ministry of Security and Justice

PO Box 24044 | 2490 AA The Hague | The Netherlands
T +31 70 888 66 66 | Fax +31 70 888 65 55

www.forensicinstitute.nl

June 2011