Information and knowledge management in intelligence situations

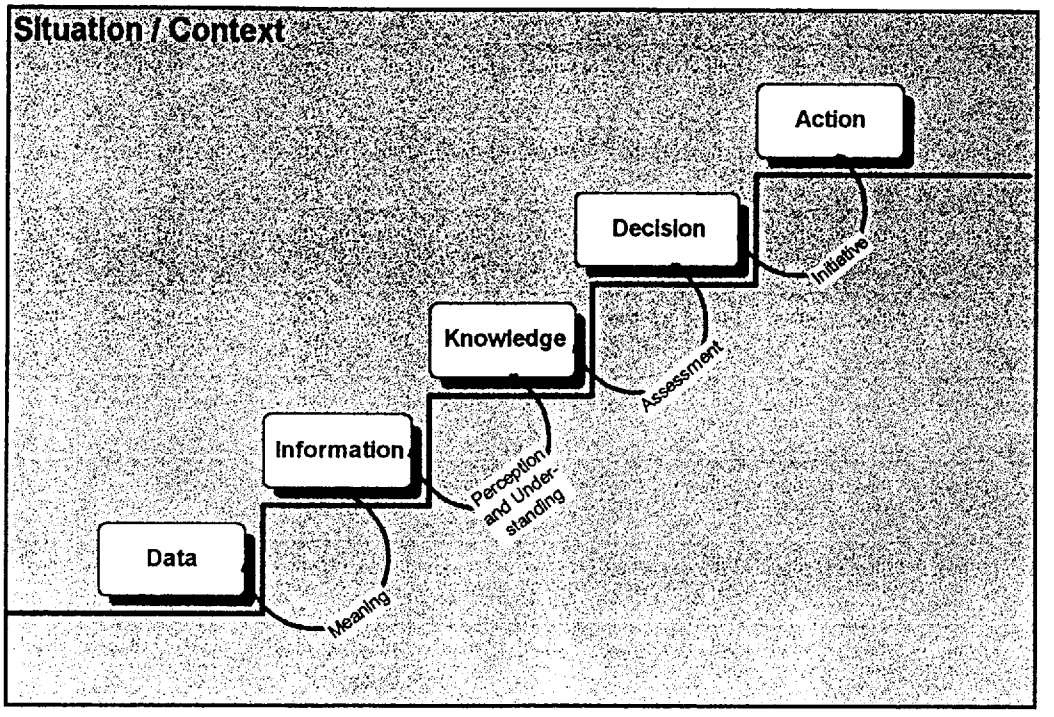
Annette Brückner

General Manager of GENESYS GmbH, Munich, Germany

Chair of POLYGENESYS, Inc., Mil Valley, CA

1 Role and position of information in the intelligence process

1.1 The Knowledge Chain



Information is only one part of the knowledge chain.

Quality accumulation from step to step

From data to information

Data "pieces" are related to each other to indicate their meaning ("Miller" = profession / "Miller" = family name)

From information to knowledge

The individual perception process:
"To know" requires to understand and to assess. Therefore knowledge can only exist in the brain of the individual.

Knowledge can be exchanged between individuals. However they exchange messages about "what they know". This information turns into knowledge within the brain of the recipient.

1.2 The informational situation

The informational situation suffers from several handicaps:

Not all necessary information is actually available. Vice versa a lot of information is available, that is not really necessary.

Assessment of information becomes difficult due to several reasons:

1. Most often information is not complete.
2. Available information becomes known in a different time sequence than it has happened.
3. Available details cannot be put into the right context. This makes correct assessment almost impossible (the "notebook problem").
4. Information having become known may be falsified.

1.3 Characteristics of an "intelligence situation"

1. Bipolar situation	Every intelligence situation is characterized by a bipolar situation: Two non-cooperating parties stand on the two sides. They are separated by an invisible wall that prevents a correct perspective to the real situation and background on the other side.
2. Active sealing off	One or the both parties actively seal off.
3. Available information	.. is incomplete in most of the cases.
Conclusion	1. Necessary information about the other side cannot be acquired by conventional investigation and information retrieval. 2. Available information relates to a lot of details; it is most often not sufficient to really "know" about the other side.

1.4 Intelligence as a method to generate knowledge and prepare decisions and actions

Intelligence is a method to derive conclusive knowledge about an "opposite side" in every situation, when complete and accurate information cannot be obtained by conventional means.

Intelligence is not restricted to specific businesses or application fields.

However, intelligence is required in any situation, when knowledge has to be generated about an opposite side that cannot be interrogated directly.

Intelligence applies not only to the "Central Intelligence Agency", nor to crime intelligence, but also to

- market and customer intelligence,
- competitive intelligence,
- and to various other fields in business and industry.

Information systems for intelligence work

Intelligence work is based on data and information.

Information needs to be stored, evaluated an, processed and exchanged. Computer systems and databases can be used for that purpose.

Information systems for intelligence workers have to fulfill the following requirements:

General Flexibility

Capability to enter any item of information and any relationship between items of information.

Hard and soft information

Capability to store hard facts, soft information and assumptions, thoughts, hypotheses, and scenarios simultaneously.

"Structured" and "unstructured" information

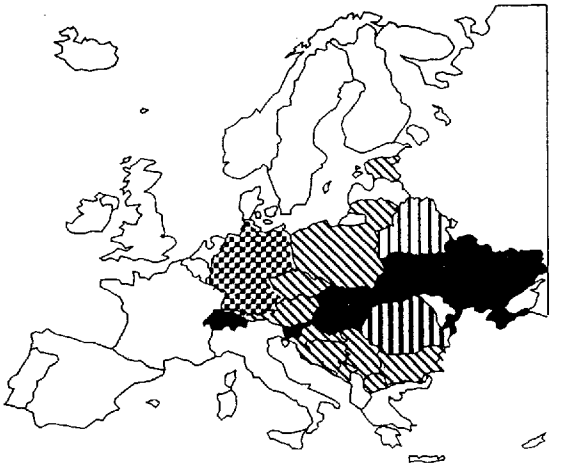
Capability to store and process structured information (that can be used for direct searches) as well as unstructured information layed down in text documents, graphics, photos, videos, sound sequences etc.

1.5 POLYGON as an information system for intelligence work

POLYGON is an information system that was dedicatedly designed to support the intelligence process.

Its development was initiated by orders from the German Minister of Interior in 1994.

Meanwhile, POLYGON is used as a nationwide system for crime intelligence in Switzerland, various states of Germany, in Hungary, the Slovak Republic and the Ukraine.



Despite of the sizes of these projects POLYGON is completely scaleable, i.e. can be used as an intelligence system on standalone PCs and departmental client-server solutions as well.

The following practice examples will demonstrate the requirements arising from different intelligence situations and the solutions possible with POLYGON.

2 Practice examples

2.1 Case Processing, Investigation and Analysis

This first example demonstrates the general usage of POLYGON

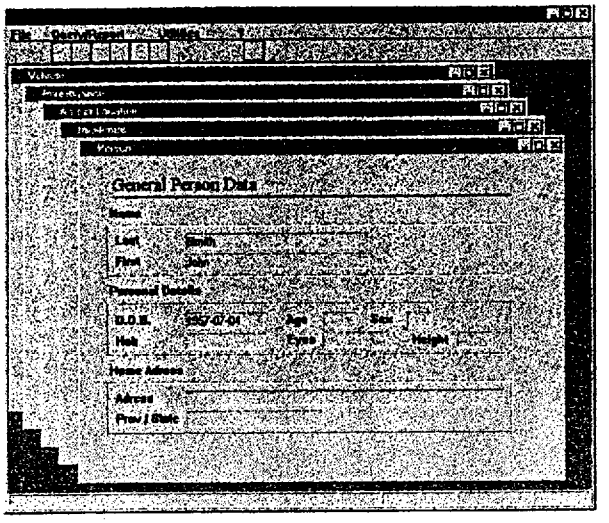
Madame-Plus Ltd. are manufacturers of high quality ladies' wear. Towards 10:40 on the night of 10.1.1997, four unknown persons break into the warehouses of Madame-Plus Ltd. and steal several sample collections, intending to make their getaway in a van. A night watchman realizes what is going on and surprises the thieves as they are loading the stolen goods. Three of the four thieves manage to make their escape in the van, the fourth in a Lancia Thema. This fourth person is shot by the night watchman and seriously wounded.

His personal details are seized and read as follows:

Michel Baudoin, born 11.10.1960 in Nancy, France, …

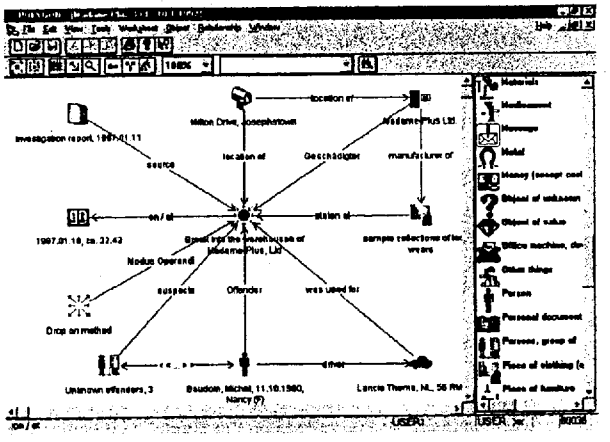
Had you been using a "structured database", ...

... your data record on the event might have looked like this:



In POLYGON, that same record looks like this ...

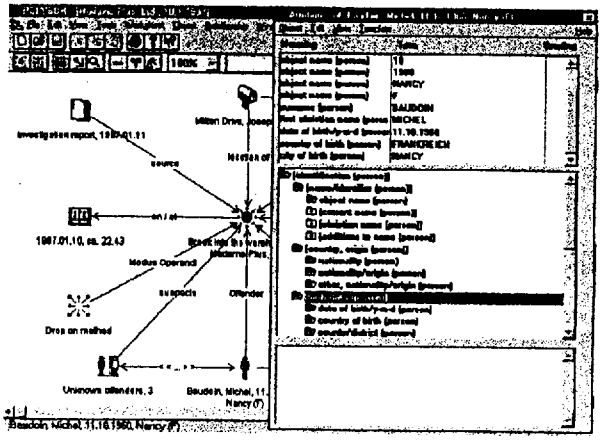
What you see here is data being entered in a database!



Each symbol or icon represents an object, an object being a response to one of the 7 principle investigative questions (who? what? where? etc.). Relationships between objects are shown by lines, each line containing a label telling us what that relationship is. POLYGON knows no limits, either with regard to the type and number of objects in the database, or to the type and number of relationships.

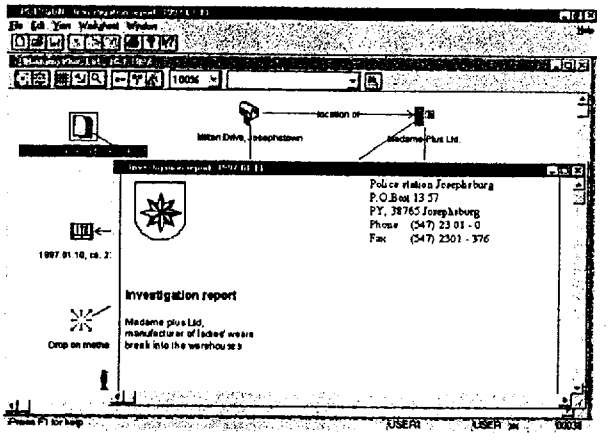
Objects and relationships are given attributes

Any number of attributes can be assigned to each object and each relationship. They serve to describe and identify an object or relationship more precisely.



Documents such as investigation reports ...

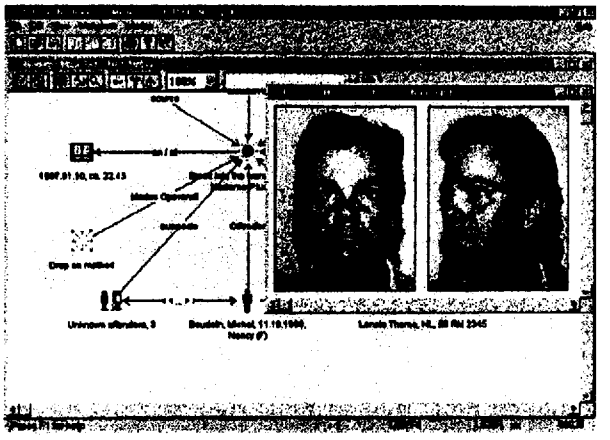
can be produced and edited directly from within POLYGON using any of the usual Windows programs. Documents too are stored in the database.



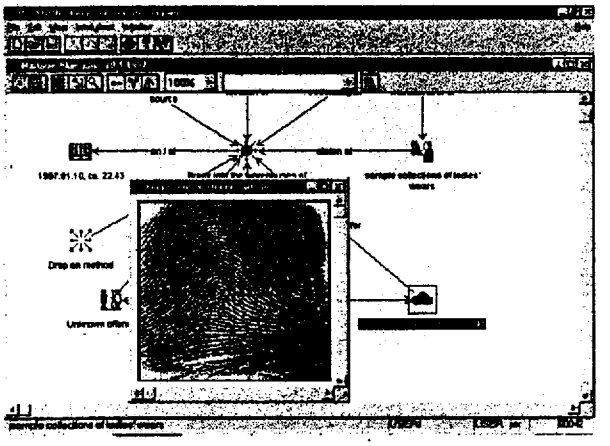
To have a document displayed, simply double-click on the respective icon (here "Investigation Report"). The document appears immediately in the re levant editor.

In place of an "electronic" document, you might want to record a reference to the scene of the crime.

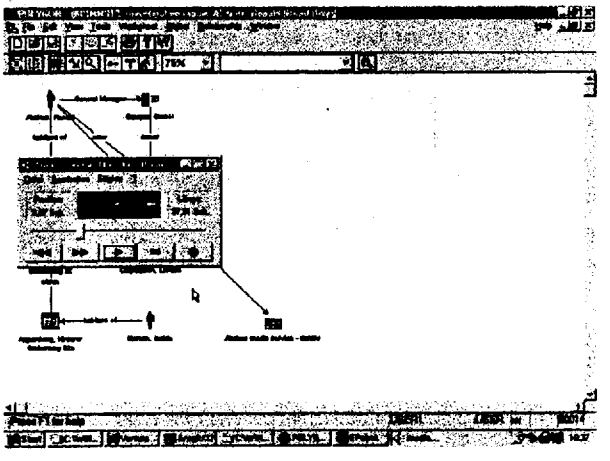
Photographs



Fingerprints



Even Audio and Video sequences



can be stored in POLYGON's database and displayed/played at the click of a mouse button.

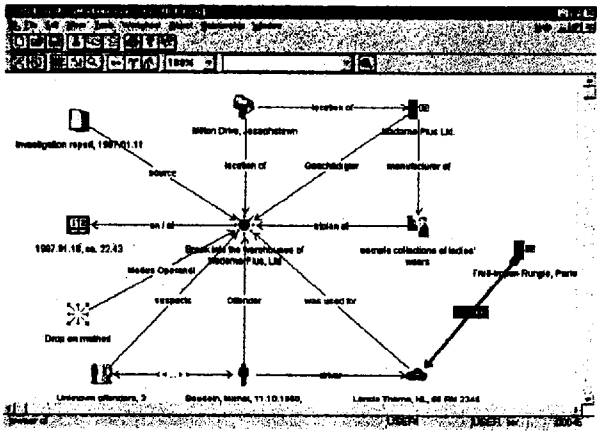
Approaches to investigation

An investigator doesn't have to spend long searching through the database. He or she simply evaluates the existing links between the various items of information:

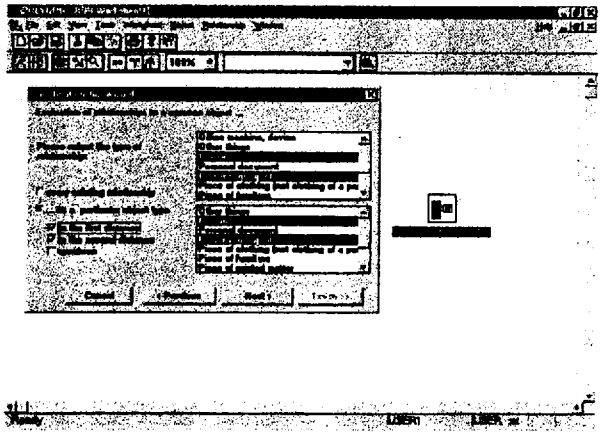
In a single work step, the investigator asks POLYGON ...

- whether it is already familiar with one of the objects. If so, he asks POLYGON to tell him
- which relationships the object has.

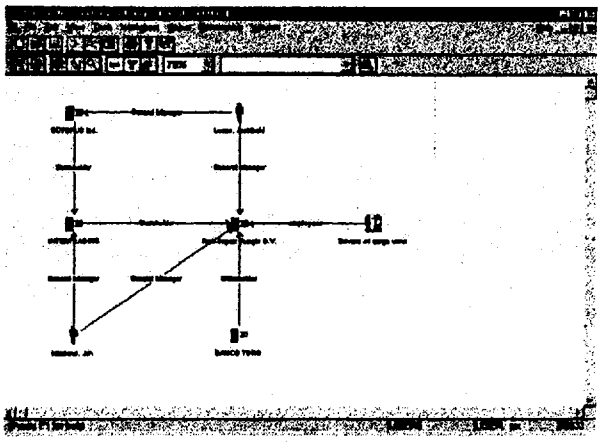
POLYGON strikes lucky:
It is familiar with the vehicle used in the escape and its owner.
POLYGON now displays the located object (owner) and creates a relationship between it and the source object.



Further evaluations now focus on the owner. Is POLYGON aware of any relationships between the owner and other persons or companies?

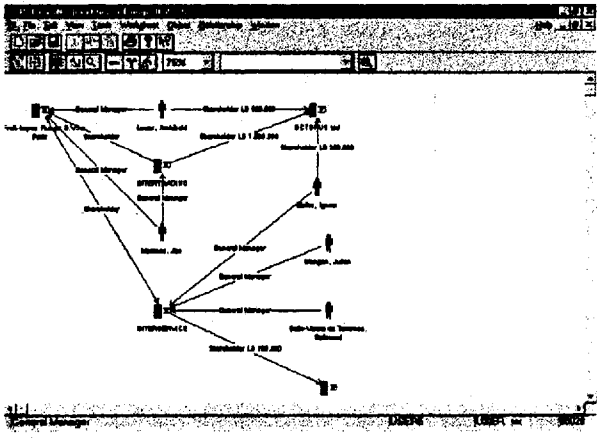


A few seconds later: POLYGON has searched through all the structured images (worksheets) in the database via a drilling down process. It now displays all the objects that have had connections with the "owner" at some time or other.



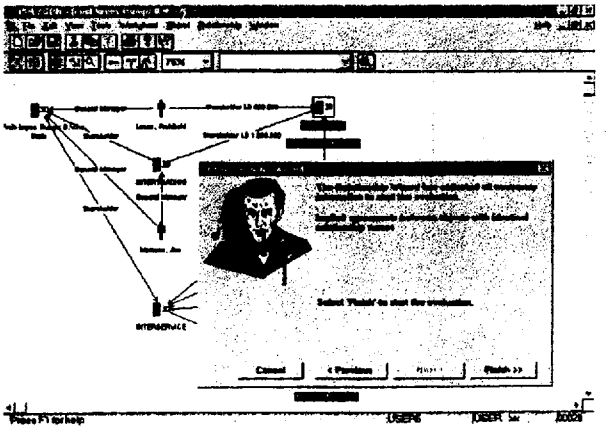
Some interesting findings are made: "Fruit-Impex" is part of a complex of firms!

The next set of analyzes ... focuses on Fruit-Impex's affiliated companies and partners.



POLYGON reveals several additional networks connecting companies and persons:

The investigator now looks at ... each affiliated company and partner separately. Again, he evaluates the links between all marked objects:



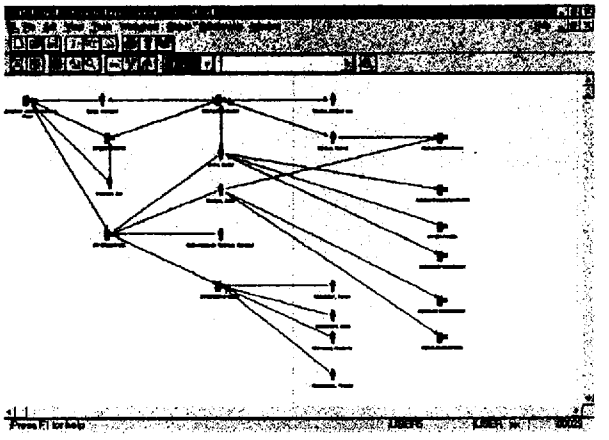
A case-oriented analysis has now become a strategic analysis ...

- What is this group of firms up to?
- Who is involved?
- What are their functions and positions?

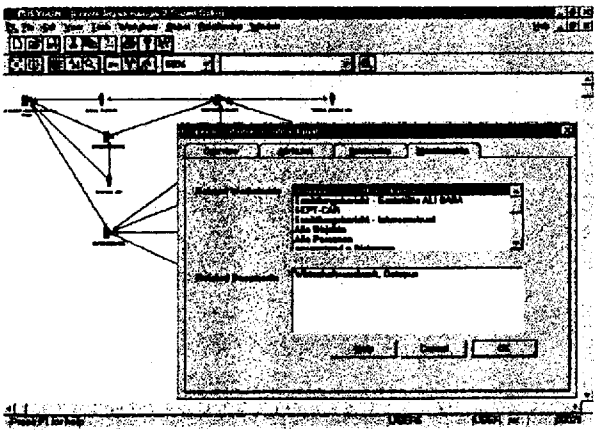
The investigator must now orient himself ...

In which context does this person appear?

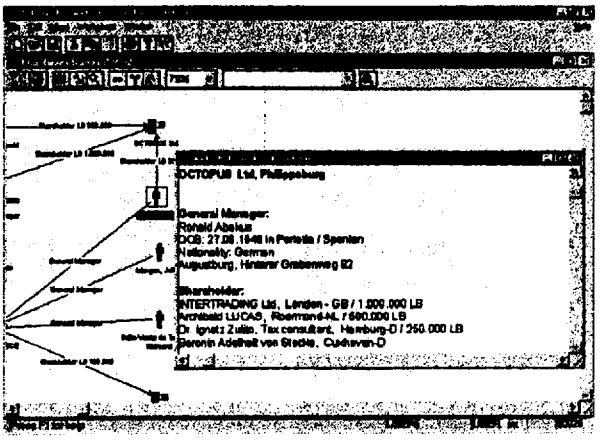
What evidence (documents) supports this?



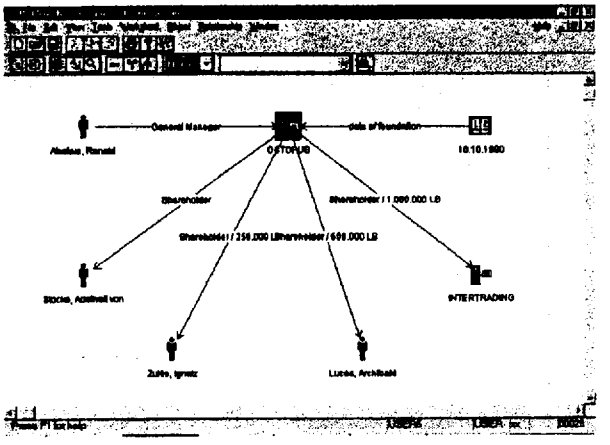
In this window, POLYGON shows all the structured images (worksheets) in which the selected object occurs. The field below shows all the relevant documents as supporting evidence.



With a click of the mouse, the investigator fetches the document onto the screen ...



followed by the connected worksheet:



Interesting! ....

He has just found some of the persons and firms listed in the case he is currently investigating.

Hypothesis

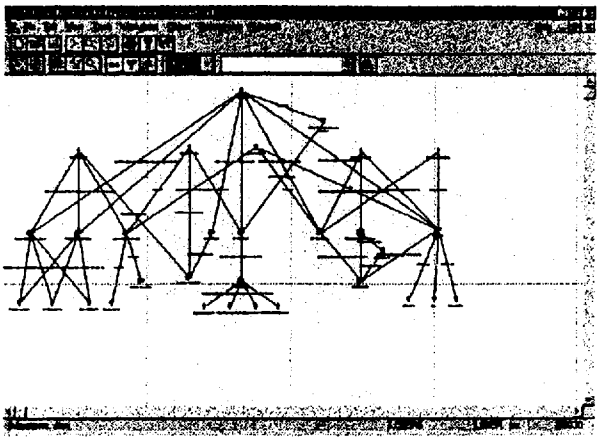
In readiness for the next situation report, the investigator formulates the following hypothesis:

"The robbery at Madame-Plus is linked to several persons and a corporate group operating on an international basis. The latest findings point to the group having a clearly organized structure, with the various members assigned different duties."

He now decides to verify this hypothesis ...

POLYGON helps him analyze the network of persons and firms.

Half an hour later, the following picture emerges:



The investigation is now moving in a new direction ...

A new, operative line of inquiry is started against the ring-leaders of the first and second levels. Further investigations target the various companies at their points of intersection.

Postscript

In a spot check carried out by Customs & Excise officers at the port of Rotterdam, a refrigerated container was found to contain several sample collections of high-quality ladies' wear. The collections were impounded. The owner of the container is a certain Fruit-Impex B.V. of The Netherlands

2.2 Example 2: Analysis and evaluation of existing databases (RISSNET)

Most often information is already available within a database

This second example will demonstrate, how existing databases (or excerpts from databases) can be imported and converted. Complex Structures which have been invisible before will then be perceivable at a glance.

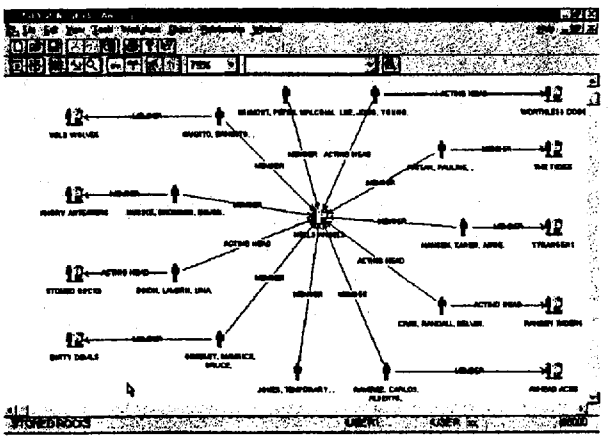
RISSNET

RISSNET provides a database covering drug and organized crime related events and correlated items such as suspects, locations, weapons, communication means etc. The database contains information from all over the United States.

RISSNET and POLYGON

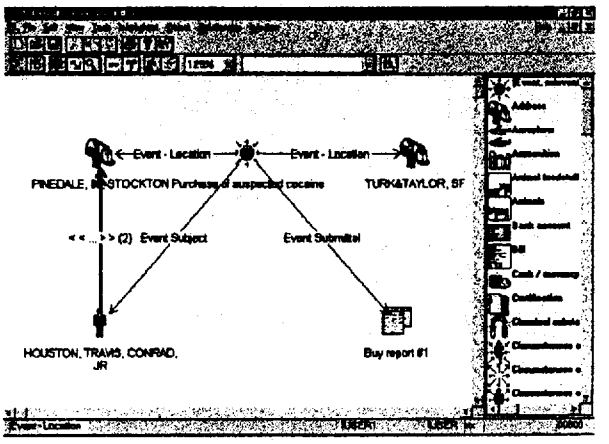
Information from the RISSNET database was converted into the POLYGON structure in order to demonstrate, how RISSNET information can be visualized and analyzed with POLYGON.

POLYGON is capable of automatically presenting information items (called objects) and all their related items in a graphical structure.

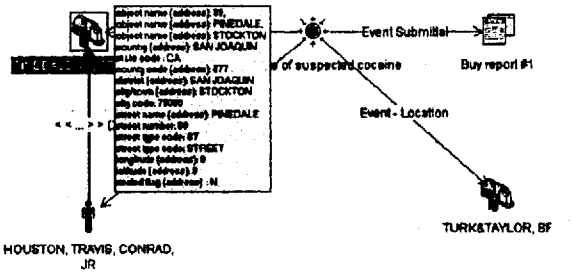


Investigation of a sample case

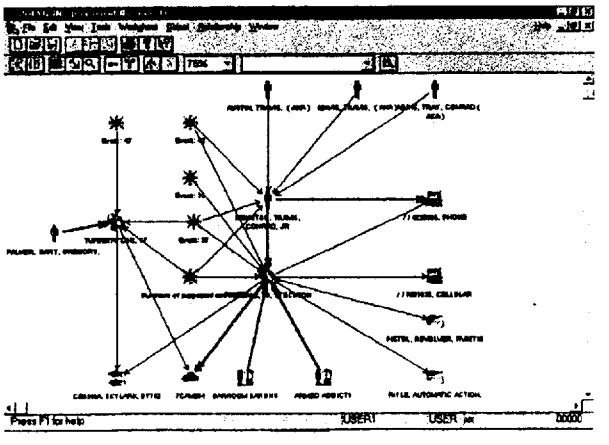
During a concrete investigation a Mr. "Houston, Conrad, Travis" comes into play.



Mr Houston is already well known. Various information about this person are available.



Information is available about the suspect and the location. As a result of link evaluation POLYGON now displays all currently existing relationships of suspect and location.



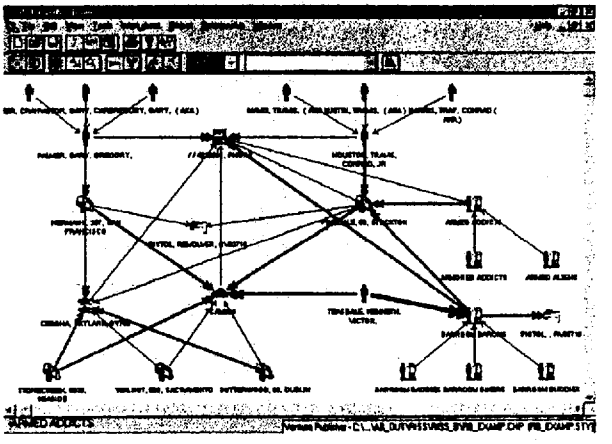
378

Further evaluations in POLYGON ...

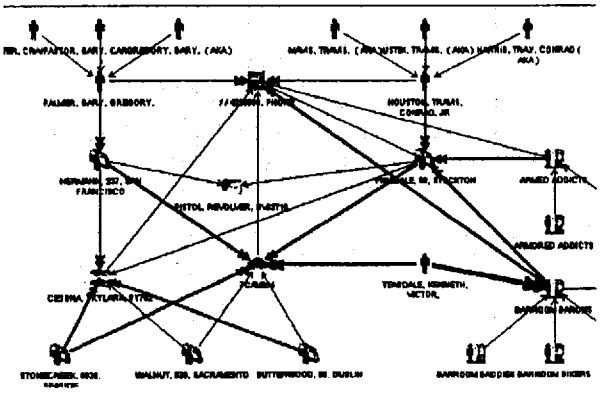
... now focus on the suspect and his environment. Is there any evidence of relationships between him and and other persons or organizations?

A few seconds later ...

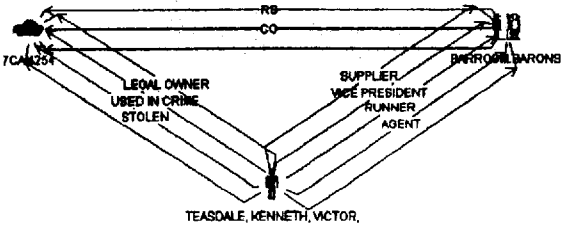
POLYGON has searched through the whole database via a drilling down process. It now displays all the objects that have had connections with the esteemed Mr. Houston jr. at some time or another.



Several direct and indirect relationships exist between he and Gary Palmer.

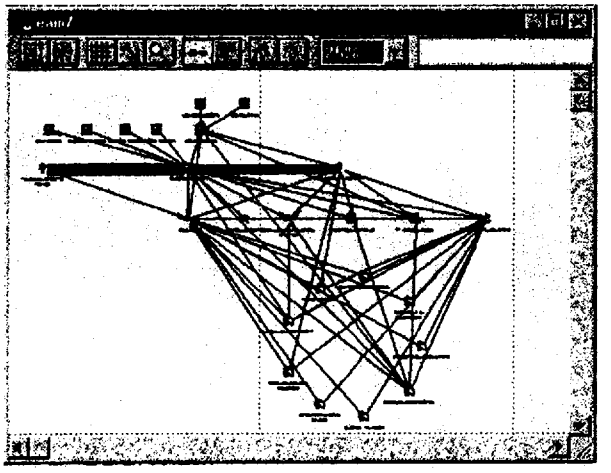


What needs to be evaluated next is the role of Kenneth Victor Teasdale, who also seems to be a major player ..



Only a few minutes later this survey shows up ....:

Palmer and Teasdale obviously jointly control an organized gang structure, which is provided with the necessary equipment of cars, aircrafts, weapons, communication means and addresses.



POLYGON produces on the next request this survey of clusters about the currently known gangs and their members.

The RISSNET analyst provides his colleagues from other associated units engaged in the case with the knowledge available at present.

Both of them are glad to have existing information available "at a glance". They eagerly wait for new information being entered into RISSNET and showing up in POLYGON ...

2.3 Example 3: Application of business intelligence to crime intelligence

The starting situation

The narcotics market of an American metropolis is in firm hands:

A lot of indications arose over the years, that the Kutun family, a Turkish clan plays a leading if not the dominant role in the heroine market. The head of the family as well as his two brothers have been resident in the city for more than 20 years. As far as is known up to now, the three brothers are directly or indirectly engaged in several companies as are restaurants, forwarding agencies, car rental and leasing companies.

Effective measurements of sealing off as well as influences to politics and public administration prevented any achievement of considerable investigation results in the past.

Recently the executive floor of local politics and police decided to undertake a last massive attempt to investigate the actual engagement of the clan members in illegal businesses.

The methodical approach

Due to the effective seal off measurements in the past further operative investigation are not considered to be successful.

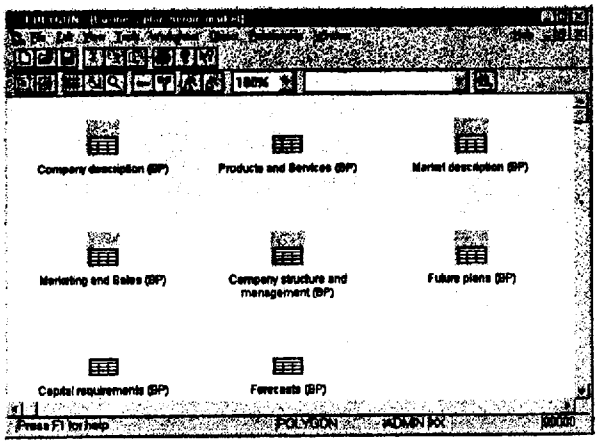
Yet a small - as well sealed off - analysis unit is installed. Their task is to analyze already existing information and indications and to work out strategies how successful proofs could be gained.

Although the members of the analysis unit have no specific computer knowledge POLYGON shall be used as a supportive tool for strategic analysis.

Intelligence Business Analysis	Since the clan has been extrememly effective in sealing off its actual activities numerous proceedings in the past didn't produce any tangible results. Therefore the analysts make up their mind to change the approach: Since available facts did not prove satisfactory evidence in the past and sufficient facts lacking up to now can probable not be investigated in the future they bank instead on "Intelligence Analysis":
Problem definition and planning	The analysts meet for a few days workshop - undisturbed by their normal daily work - and define the attainable and desirable targets: • Proof of the involvment of the individual clan member ... • in crime offenses generating long imprisonment and / or • smashup of the "company structure" of the opponent. In order to temporarily substitute lacking factual information they will create scenarios about the past, present and future situation of the clan by applying plausible considerations about its behaviour in business. Scenarios shall then be used to derive specific investigation missions and to settle the basis for further analysis steps.
Definition and acquisition of necessary information	
Collation, Analysis, Estimation, Prediction	Basic assumptions for the scenario The analysts discuss about the most probable real motive ot the clan: Ethnical, ethical and political reasons are excluded after a short discussion: It can be basically assumed, that the family members act on pure financial reasons!

Creation of a hypothetical business plan

Police analysts temporarily turn into "business men" who put themselves into the position of the family: In a joint action they draw up a hypothetical business plan for the clan and work out step by step the plausible and necessary components and their correlations.

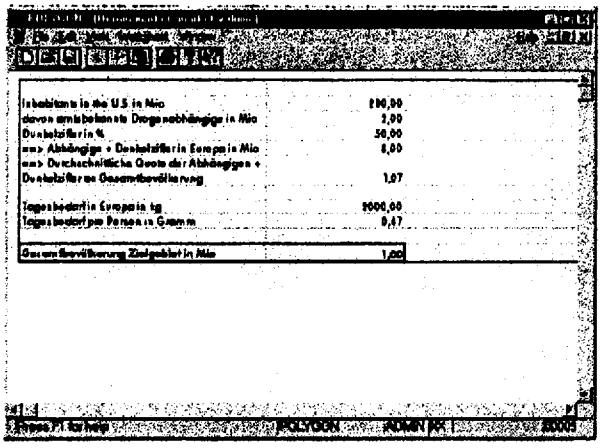


Resistencies have to be surmounted

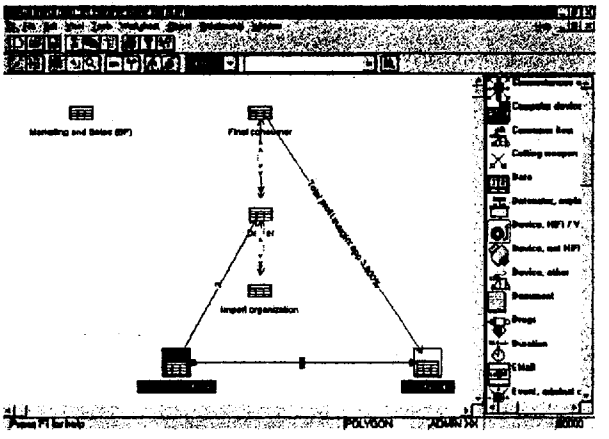
Criminalists being old hands at dealing with hard information need to learn that also soft information, assumptions and hypotheses can effectively be included in the investigation and evaluation process. Up to now they were used to keep these things at the back of their minds. All of a sudden they are faced with POLYGON which is capable to deal with hard as well as with soft information.

They continue their work on the hypothetical business plan:

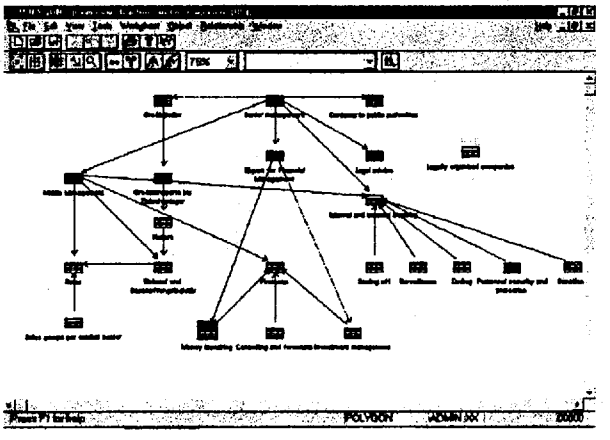
They carry out commercial calculations about the potential market size (and get frightened at the actual volume of almost 60 mio USD per year),



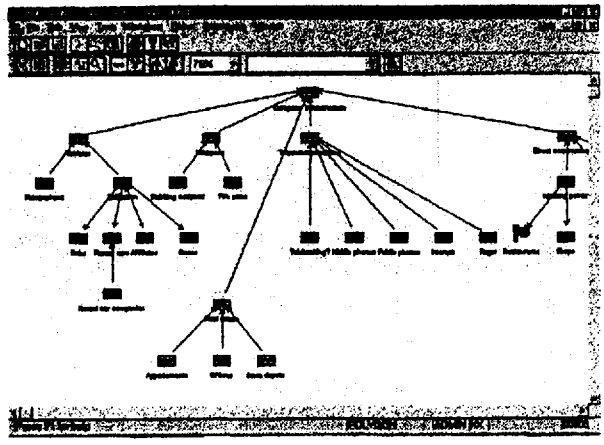
derive the potential profit margin,



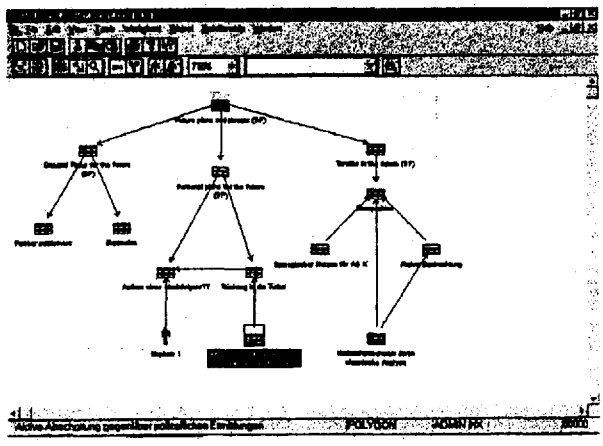
define the necessary infrastructure for such a business,



analyze the necessary and plausible structure of organisation and management and



create hypothesis about future activities of and threats to the gang



Knowledge

While cooperatively working on the business plan each of them makes the astonishing detection that every single one of them has a wealth of detailed facts at his disposal which suddenly can be integrated into a plausible context and suddenly "makes sense". All these available facts are included in the scenario.

Only a few days later the "business plan" is ready. It's structure is very detailed, the components and their correlations fit plausibly together and it contains a wealth of detailed information derived from the brains of the few analysts.

The analysts totally agree what makes their approach different from the attempts in the past: While past investigations were settled upon and tried to derive meaning from available facts they try it the other way round: They start their analysis at the supposed target and reconcile the available facts with this target and derived activities.

Back to information acquisition	The scenario compiled up to now defines the next tasks: There are a lot of files in the office which have to be repeatedly checked with concrete questions. Yet the job is troublesome, sometimes tiring and time consumptuos. Files have to be evaluated page by page, existing fact information have to be entered into and correlated within POLYGON.
The current status is presented at the directorate	A beamer helps tp present the current status of analysis and investigation directly from out of POLYGON: The deputy chief talks about a "new quality of information management and analysis". Actual results are so convinving, that the team gets the order to continue its work. A personnel enhancement is to be considered ...

PROCEEDINGS 1998 7th International Conference & Exhibit OPEN SOURCE SOLUTIONS: Global Intelligence Forum - Link Page

Previous	OSS '98 Nate Boyer, Commercial Imagery Support Options: Trade-Offs and Value-Added,
Next	OSS '98 Robert David Steele, Information Peacekeeping: The Purest Form of War (JMITC Lecture Outline),

Return to Electronic Index Page