

Visual investigation tools show crime connections

By Keith Newman

Businesses, government departments, law enforcement agencies and private eyes engaged in criminal investigations are finding it increasingly difficult to make sense of the deluge of data unless they have specialised software to isolate patterns and connections.

Manually sifting through thousands of pieces of evidence is proving hugely inefficient, particularly in complex fraud cases or crime scene investigations and while computer systems are essential they can add to the information overload.

Increasingly investigators are turning to dedicated software systems that enable data mining and pattern recognition that uncover links between disparate data to transform the way they go about their business.

Paul Stokes the General Manager of Methodware, a risk management company wholly owned by Christchurch software developer Jade, says the problem with many law enforcement agencies is they need to engage their intelligence people to get any kind of mapping, timelines or linking done.

He says people would be surprised if they knew the number of agencies in this

country that still use paper to manage complex cases. "A murder or serious crime investigation might run for 12 months and involve hundreds of thousands of pieces of evidence."

And while it's great to be able to sift through data and come up with patterns and links on a computer, he says knowledge presentation is just as important, particularly if you can drag a timeline across to show how events built up to a crime.

"This can be crucial in whether a criminal is caught, however there are nowhere near as many intelligence people as there are operational people so you end up with these huge backlogs of work," says Stokes.

Connecting the dots

While data mining and association software has been around for years, next generation tools are able to uncover hidden links and graphically display a wider range of associations between people, places, times and events — even mining social networking sites for clues.

Jade Investigator, developed six years ago for the Australian Federal Police (AFP), gives operational people the tools to make important connections across masses of data and simplifies the management of large teams, tasks and case updates.

Such a system can show the relationship between phone numbers, people and locations. "You click a button and it'll draw a link showing you all the people, places, objects and entities and how they're linked together," says Stokes.

If that evidence remains in paper files only one person can view the data at a time. "You can miss a lot of things and it slows down the investigation," he says.

Jade Investigator, a big export earner for Jade Software, was recently 'performance

tuned' and made more scalable for larger organisations. It is now used by 70 law enforcement agencies in 16 countries; including the largest such agency in the UK.

Local users include the Government's Pacific Prevention of Domestic Violence Programme and the Pacific Transnational Crime Network.

It's already out there

There's a vast array of useful information in the public domain that can be used as a resource for Police, employers, private investigators and others, including driver's license, vehicle ownership and the phone book.

Now the exponential growth of voluntarily uploaded personal information on the internet has made the investigator's life much easier.

"Social networking is a massively growing area of data where you can see who's connected to who. I don't think people understand how much data they make available about themselves," says Dave Ashton, Business Development Manager for i2 Asia Pacific distributor, Visual Analysis.

While i2 Analyst Notebook doesn't directly enable interrogation of this data, there are companies that produce plugins to drill down and look into social networking sites like Facebook and Twitter to find links between people.

Ashton says software developers and investigators have to use any means possible as the criminal world does not rest in its ability to commit fraud or by-pass the rules. "As soon as they're caught doing one thing they change to try to keep ahead of enforcement, so it's essential to get accurate, quality information which is the key to a good investigation."



Paul Stokes, General Manager of Methodware



Ron McQuilter, Chairman of the New Zealand Institute of Professional Investigators (NZIPI)

Ron McQuilter, Chairman of the New Zealand Institute of Professional Investigators (NZIPI), says social networking is “huge” in the data it provides to his industry and not just for tracking down fraudsters and other criminals.

He’s recently found it “an incredible help” locating people who are owed money from a 20-year old scheme which is in the process of being shut down. “I’ve managed to track down a number of these people on Facebook to tell them the good news from the comfort of my desk.”

While that’s a relatively simple use of existing technology, the combination of what can be gleaned from social networks and data mining or association charts that cross match information from different sources, is changing the way private investigators operate.

Picture tells a story

McQuilter says around 15-years ago there were few people in the country who could use this type of technology because it was so complex and expensive. Today it’s more affordable and has a more intuitive dashboard format.

A number of packages are in use including i2 Analyst Notebook which he says is the most popular. Although it’s costly, he’s moved from outsourcing to in-house ownership at his Paragon agency, largely because of the value of being able to produce easy to understand charts.

“You just have to see the pictures to believe it; the big charts you can put on a wall are like a work of art. It’s very clever from an investigation point of view.”

Several companies, including Intelligence Solutions, outsource this kind of software at an hourly rate which McQuilter suggests “is probably cheaper than a PI would charge.”

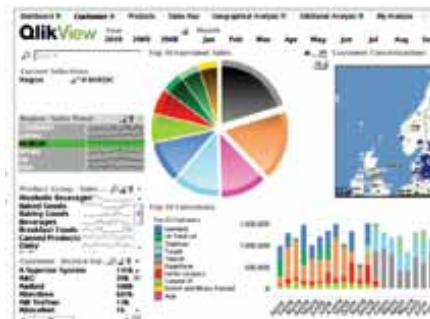


i2 Analyst Notebook is one of the new suites of tools that can create clear charts from complex data

They use electronic data or pick up piles of hard copy, key in the relevant fields: company names, directors, shareholders, date of incorporation etc, then ask the software to discover relationships and links.

Another product coming into common use for investigations is reporting, analysis and business intelligence tool KlikView. “Put in raw material sucked from different spreadsheets or digital sources and it’ll search through it for associations,” says McQuilter.

In the ‘old days’ this capability was only in the hands of the big five accounting firms who did forensic analysis and data mining. “It used to cost \$100,000 to sift through all your accounts, payables and cheques looking for associations, now it’s affordable even for a PI. It’s making huge inroads for a fraction of the cost.”



KlikView, a data mining tool that brings high end analysis to the desktop

Heading the investigation

While New Zealand Police make good use of i2 Analyst Notebook, official investigations can also be triggered through evidence provided in this format by private investigators, corporations, banks, insurance companies and auditing and accounting firms.

The Windows-based visualisation package can be used at an enterprise system level or de-coupled to a laptop for remote or field work. It uses link analysis in the search for connections across masses of documents including bank records, claim forms and telephone call records.

If you want to see who called who it can rapidly process thousands of call records and run a timeline. As patterns emerge you can put people in places and see where events overlap or coincide. The resulting trail of evidence can then be depicted in a series of ‘charts’.

Dave Ashton, who first encountered i2 Analyst Notebook while working in military imagery intelligence and forensics for the UK Royal Air Force, says local sales have been on a growth curve over the past 12 months.

NZ Police, the military, banking and insurance companies and government agencies and corporates use it, and many have recently upgraded to version 8.7 which features a different kind of ‘social network’ analysis.

This scans for connections between people, for example determining who the kingpins are in a fraud network, a crime syndicate, drug cartel or a gang.

“Generally some person has more influence in a network and you can quickly track that through their associations then focus attention on those individuals,” says Ashton.

“It’s a bit like analysing degrees of separation. If I have a bank account and I transact money into someone else’s account and they make payments to others, everyone’s connected by those transactions.”

Another feature in the latest version can uncloak hidden IP (internet) addresses to detect cybercrime, such as IP mapping where computers are linked together into botnets to launch attacks on other sites.



Dave Ashton of Visual Analysis

And while criminals often use software to hide their IP addresses, the i2 software can isolate groups of networks using link analysis and identify where attacks are coming from. It's a little more complex than identifying perpetrators of fraud or financial crimes, but the same principals are applied, says Ashton.

Jade digs deeper

Jade Investigator is mainly deployed to enhance and manage the operational side of fraud and crime investigations; now developer Jade Software is leveraging its expertise to launch a specialised analytics product later this year.

Joob Intelligence can extract data from a range of sources, including social networks, using advanced analytic techniques such as text mining, an intelligent rules engine using fuzzy logic and machine learning.

It provides detailed background information, patterns, links and connections that can be used in conjunction with operational focussed software. Once the evidence is gathered and graphically mapped it can be passed on as 'an incident' in Jade Investigator.

When operational officers have completed their allocated follow up tasks and the workflow is complete, a 'brief of evidence' that is admissible in court can be handed to the prosecutor.

The Joob suite uses timeline analysis and network visualisation to deliver a more intuitive view of complex data for law enforcement, financial services companies,

government agencies and border control for example.

Joob could cut through the swathe of immigration paperwork by electronically extracting data from flight manifests, visas and related forms and documents, including checking whether a person has another passport or has signed documents in another name.

Paul Stokes says it's a very complex thing for a computer to extract meaning, so 'entities' are created for sentiment analysis. "We can look at someone's Twitter feed and the computer can tell us whether this is positive, negative or neutral, and in context with everything else in the sentence, whether it's angry or happy."

When clustered with other things a person might be saying, Joob can establish patterns.

If the word 'bomb' is used and a known associate uses 'explosive' it can help isolate persons of interest.

If a person recently made a comment of concern on Twitter to someone in a country the government is not happy with, an alert could be generated in real time so officials prevent them boarding a plane.

Smart fuzzy features

The system's advanced rules engine enables businesses and agencies to write rules to identify criminal activity. While specific rules can never pre-empt something unknown, Joob's fuzzy logic enables the technology, based on behavioural changes, to make up its own silicon mind.

"Machine learning systems have the ability to learn from the data they're examining and adjust the rules into patterns of detection to find new things as they happen," says Stokes.

While banks are required to notify the financial intelligence unit of the Police if more than \$10,000 goes across the counter, smart criminals might split that into smaller amounts over a period of time.

A simple rule wouldn't find that, although a more intelligent rule might flag the fact that over a three week period smaller amounts were deposited by the same person at different banks. "This makes it much harder for criminals to break up their activities to try and beat the rules," says Stokes.

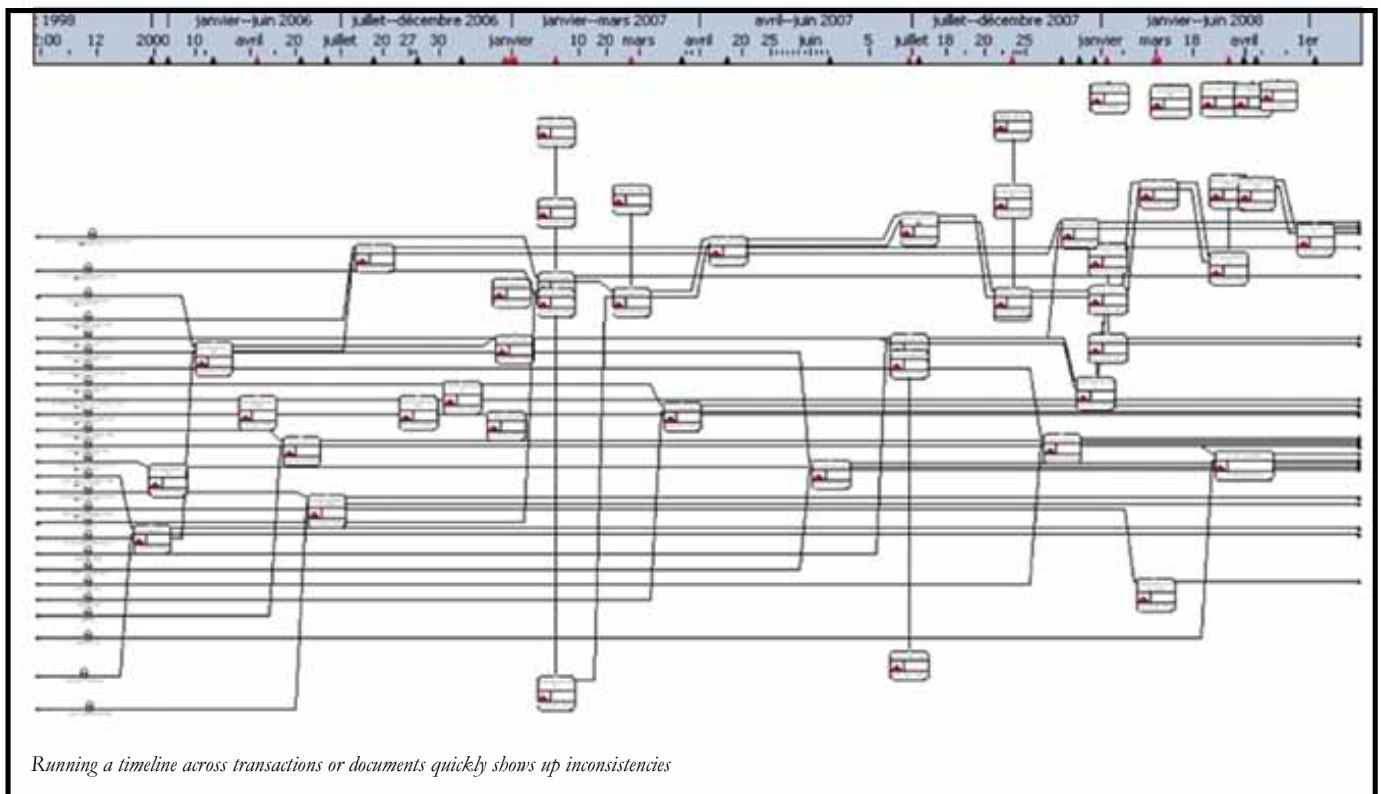
Another area where there's a growing demand for this new generation of smart tools is detecting employee fraud; narrowing down the 'how, where, when and who', if stock or funds are going missing.

Data can be gathered in real time from building access systems to determine who is coming and going and where they are at any time as well as keeping a log of who goes into certain parts of the corporate intranet.

Through scanning all these records it could help identify when goods were going missing, who had access to the stock room, or who might be downloading company secrets or staff lists to pass on to recruitment agencies or head hunters.

Auditing for oddities

The big auditing, accounting and financial services companies typically have



Running a timeline across transactions or documents quickly shows up inconsistencies

specialist departments using this kind of technology to investigate various types of fraud, now private investigators can be similarly equipped.

“If a company suspects fraud they may supply a private investigator with the appropriate data and after this has been processed their case notes could form part of a formal police investigation,” says Dave Ashton of Visual Analysis.

He says one un-named New Zealand Government department installed the i2 Analyst Notebook two years ago after realising they had a problem. “They soon became aware of significant fraud activity which they were able to isolate.”

The same approach has saved insurance companies megabucks by identifying irregularities and possible links, without the need to manually sift through copious amounts of paper work.

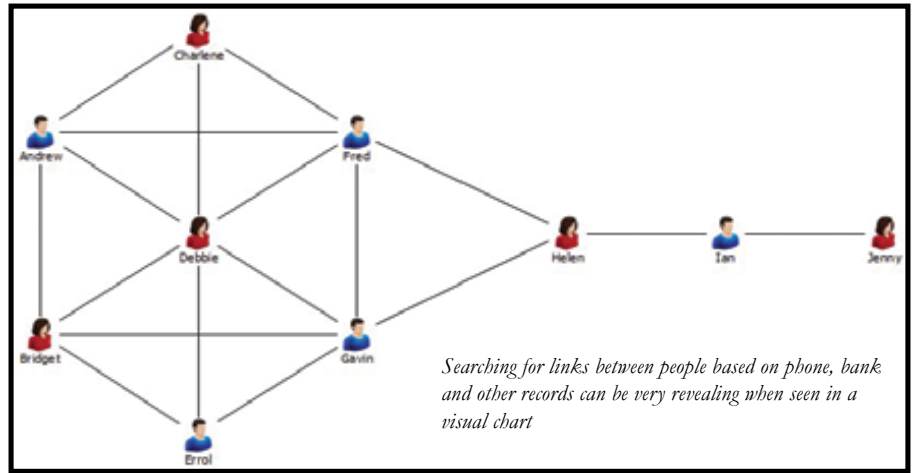
Lumley General Insurance New Zealand, recently acquired Analyst Notebook, and in one of its first major successes uncovered a fraudulent claim exceeding \$300,000.

Through applying several analytical tools, the company’s fraud team identified a number of discrepancies and created a ‘sequence of events’ chart to identify the time and date of activities undertaken by the insured.

This was then organised into specific themes in a ‘statement analysis’ chart. As a result key pieces of information provided by the insured and other parties helped firm up the discrepancies, resulting in the claim being declined.

Dave Ashton says, with limited resources and large volumes of claims it’s hard to see where the same person’s details come up, as fraudsters often change the spelling of their name or use different addresses to make claims look unique.

Instances have been uncovered where multiple claims are made for the same work or insurance company staff recommend a particular sub-contractor for certain kinds of work and then pay money into a personal account.



Searching for links between people based on phone, bank and other records can be very revealing when seen in a visual chart

Identifying relevant images

Object and image recognition is often part of the analysis product set, including technology that can help make sense of what is happening in CCTV footage.

Checking footage leading up to a specific event or identifying certain kinds of activity can be particularly helpful in investigations.

Paul Stokes of Jade/Methodware suggests those poring over hundreds of hours of footage from CCTV coverage of the London riots might benefit from such cognitive intelligence.

“If the system was able to sift through ordinary footage of people walking down the street and only isolate fighting, breaking in and stealing or someone carrying a big screen TV down the street it would make the process a lot simpler.”

When NZSM called, Ron McQuilter of Paragon had just completed an analysis on a number of different CVs an individual had supplied to various companies in job applications.

Running a timeline over the data is a certain way to uncover discrepancies about what a person says about themselves and what previous employers said they actually did.

He says, the same technology can also be invaluable when looking for links between people involved in “companies, trusts, entities and properties” and money flows.

Another recent case would have required “10 Eastlite folders of stuff to try and explain what was going on but when you see it on a chart it’s phenomenal a picture says a thousand words.”

“If you are dealing in reasonably complex frauds, or a case where there are a lot of transactions or people being scammed, you can’t do it without some sort of association technology or chart,” says McQuilter.

All of this is a far cry from the display boards with string and coloured pins linking photos, suspects and scenarios still used by some agencies.

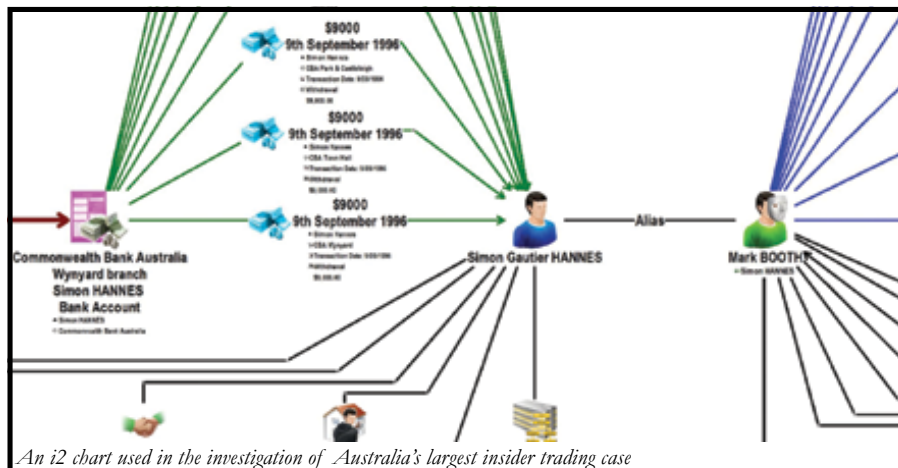
A lot of what happens in investigations has been exaggerated, glamorised and turned into a form of science fiction entertainment by TV shows such as CSI and Bones.

While it’s still some way off for DNA and fingerprint analysis to be delivered in hours and footage from all available CCTV cameras and cross agency databases searched in minutes, progress is clearly being made.

Ironically digital technology and the internet long ago made a mockery of physical borders and jurisdictions and put tools in the hands of criminals that are often far more sophisticated than those used by a many investigators.

It makes sense then, that a new generation of investigation tools, combining data mining, machine learning, pattern detection, and social network, sentiment and link analysis, should be enhancing the intelligence of those tasked with countering criminal activity.

While the cost of high-end investigative suites is still prohibitive for many small to medium operations, you can be certain cut down versions will eventually hit the market. In the meantime third parties are outsourcing their services and skills and pay as you go elements are appearing online.



An i2 chart used in the investigation of Australia’s largest insider trading case