Enhancing white-collar/commercial crime investigations using Technology

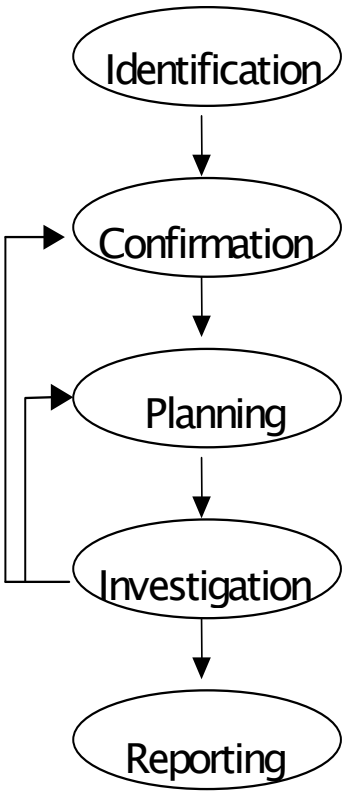
Robert Cameron-Ellis
Partner: Deloitte & Touche Forensic Services

Sani Gildenhuys
Senior Lecturer: University of Pretoria

The ever-increasing complexity of the commercial world has resulted in auditors being called upon more and more frequently to provide "forensic" assistance in investigating white-collar crimes. The investigation of these crimes ranges from simple enquiries and interviews by a single person over a few days to complex investigations by large, multidisciplinary teams, spanning many years.

This article discusses the use of technology to enhance the quality of investigations into white-collar crimes, of those investigations that are mainly based on paper documents and on interviews. It does not discuss the investigation of so called "computer crimes" where technology is used to perpetrate the fraud.

The basic stages of any investigation are:



- **Identification** – This is the stage where the first suspicions surface and preliminary evidence suggests that an investigation may be warranted. The identification of possible criminal activity in the past was mainly through internal controls, tip-offs and accidental discoveries.
- **Confirmation** – To avoid unnecessary expenditure the investigator should, *before* embarking on a full-scale investigation, confirm the suspicion by conducting a preliminary investigation.
- **Planning** – The investigation is planned with the client's objectives in mind (e.g. recovery, disciplinary hearing, civil or criminal litigation). The availability of skills and technology, timing, and geographical distribution should all be taken into account. Planning includes identifying the crime scenarios and the ranking of these scenarios in order of importance. Scenarios are the various ways in which a crime or transgression could have been committed. The evidence to be collected during the investigation is in turn determined by the elements of the crime and the *modus operandi* that was followed.
- **Investigation** – During the investigation documentary and electronic evidence is collected and interviews are conducted. This information is then combined, examined and inferences drawn for the report. New suspicions and circumstances may surface during the investigation. These might lead to a

restatement of the investigation objectives and to a replanning of the investigation.
- **Reporting** – The relevant facts, documents and other evidence is assimilated and presented in the final report for feedback to the client. This report could then later form part of the evidence for court proceedings.

The three areas of an investigation that benefit most from the use of technology are identification, investigation and reporting.

Quicker identification of suspicious activity

The detection of fraudulent practices in the past was mainly through internal controls, tip-offs and accidental discoveries. Often management would have a 'gut-feel' that something was amiss in their organisations, but they could not quite pinpoint the problem. Now, with advances in technology, fraud investigators at least have a fighting chance of finding the needle in the haystack.

Using electronic data to find footprints of fraud

Hidden within an organisation's electronic data is an extraordinary wealth of mostly untapped information. Examples include:

- false identity numbers which may indicate ghost employees;
- suppliers and employees with joint telephone numbers and addresses which could indicate undeclared interests of employees in suppliers;
- duplicate invoices and payments;
- transactions after hours or with unusual authorisation patterns, and
- transactions with unusual characteristics such as payment before the order date.

To extract these potential indications of fraud, the investigator must:

- analyse the specific organisation's risk for fraud and other 'white-collar' crimes;
- determine what 'footprints' these crimes could possibly leave in the organisation's computer systems;
- collect data from the different (mostly incompatible) computer systems and clean the data so that it can be properly interrogated;
- programme queries (tests) using software such as ACL, IDEA, Lotus 1-2-3, Microsoft Access, Oracle, SAS or SQL , and
- interpret the results.

The sheer number of exceptions normally produced by a data analysis can be daunting for the person tasked with the follow-up work. Joining the results of a combination of selected tests gives a better indication of where the footprints of fraud may be found. For example an employee with a false identity number, no medical claims, no overtime and no leave taken, is much more likely to be a ghost employee.

ACL markets a fraudsters tool kit, with pre-programmed procedures to identify suspicious activity. Taking this principal one step further, Deloitte & Touche

developed D&Tect© that contains an international library of pre-programmed, risk rated tests and data cleaning procedures. The combination of their forensic expertise and management's own insight into their particular business, together with the client organisation's data and other public information incorporated into D&Tect©, produces astonishing results.

Using data mining to find new patterns of fraud

Data mining is the use of a combination of artificial intelligence, statistics and database techniques to discover 'hidden nuggets' of information. For example, when the banks applied data mining to credit card transactions, they found that a number of large transactions followed by the purchase of fast food and petrol, indicated a stolen credit card – even before it was reported!

SAS® Enterprise Miner™ is an example of data mining software available and supported in South Africa. Such advanced technology, however, normally comes at a high price, and requires specialist training. For medium and smaller companies other options, such as buro processing, can be arranged.

Using Benfords Law to find false numbers

Being creatures of habit, people and therefore fraudsters, unknowingly use certain digits when creating fictitious amounts. Others try to 'outsmart' data analysts by using truly random numbers.

Frank Benford found that the digit frequency of certain lists of numbers can be predicted using a logarithmic formula. The digits in an accounting population do not follow a random pattern! For example the First Digit formula predicts that the possibility that the first digit of a number is '1' is 30.1%, while the possibility of '9' is only 4.6%.

Bedford's formulas are pre-programmed into software such as ACL. Investigators can also easily analyse the digits themselves using spreadsheets such as Microsoft Excel.

An example of a First Two Digits analysis can be seen in the chart below. Further investigation of the 'lone spikes' might indicate misuse of authorisation levels, or illegitimate transactions.

Benford's formulas blow the whistle on unsuspecting fraudsters by identifying additional suspicious transactions.

Enhanced investigations

Indexing and tracking paper evidence electronically

The investigator's report may be used in civil or criminal litigation. To ensure admissibility, compliance with the rules of evidence in the evidence gathering process is critical.

The rule of best evidence requires that when the contents of a document are disputed, the document must be produced in its preserved, original condition. Copies are permissible only under certain circumstances. A properly documented chain of custody ensures that documents handed in to court can be authenticated.

The rules of evidence require documents to be appropriately identified and that a record to be kept, with details of the date, by whom and from whom they were received, as well as where they are held for safekeeping. Whenever evidence leaves the investigator's control, the record should be updated.

Although a manual record may well keep track of evidence, commercial investigations normally gather huge numbers of documents. Locating important documents as the investigation expands and evolves is critical. An electronic database or spreadsheet will facilitate this by allowing key word searches. The database allows events to be listed chronologically or by witness without reverting back to the documents. The minimum fields required are the document number, document date, source, subjects referred to and a brief description.

Immediate access to evidence through document imaging

Large forensic investigations might involve several rooms full of documents. Reading through all the documents, hoping to identify relevant information is a haphazard approach at best, not inspiring a high degree of confidence. Investigators can be excused for feeling 'snowed under' by such a paper avalanche.

Imaging is the process of electronically scanning text documents and storing them on a computer hard drive or CD. These images, or pictures, must however be converted back to text to enable the investigator to search the documents for key words. This conversion process is called optical character recognition (OCR). Many imaging systems, such as SUPERText, allow additional input for each document such as reference number, key fields, date, type of document, source and author.

Some of the benefits of imaging the documentary evidence are:

- the ability to quickly search and find specific documents in the investigation, to prepare for interviews and even while in court. These searches are normally based on 'fuzzy logic' that greatly improve the probability that a particular document can be located despite misspelt words, case sensitiveness or OCR inaccuracies;
- evidence is much better preserved. There are no changes to the original document that could potentially affect its admissibility. Other evidence, such as fingerprints on the document, is also conserved. The chance that the original might be lost or misfiled is reduced.
- multiple investigators can simultaneously work on the same document, and
- huge savings in photocopy costs, not only to the many investigation team members, but also for disclosure to the defense team.

Electronic investigation diaries

Over and above indexing the evidence, the evidence gathering process also should be property documented.

It is difficult to reconstruct the events and actions months and years after the investigation, when the matter is finally presented in court. Notes made during or shortly after the events are much more credible to the court than reliance on the investigator's memory.

An investigation diary, containing a short, dated summary of every incident during the investigation, should therefore be kept. This diary includes summaries of interviews, telephone conversations, site inspections and document seizures.

Using a database or spreadsheet, to electronically document the diary for larger forensic investigations, facilitates the investigation process by:

- enabling the diaries of multiple investigators to be combined into an investigation chronology;
- keeping tabs on the total progress of the investigation, and
- helping with the drafting of the final report.

Using computers to make sense of large amounts of information

Most paper based forensic investigations contain such a plethora of information that is extremely difficult, if not impossible to assimilate without the use of a computer.

Some examples of computer aided analysis include:

- total reconstruction of records from physical documents such as invoices and receipts, using accounting packages such as Quickbooks; and
- capture of investment statements in foreign and local currencies with graphs of actual returns in comparison with the returns promised to the investors, using spreadsheets such as Microsoft Excel.

Finding the hidden relationships between individuals and entities can often make the difference between success or failure on a case. Employees can for instance be directly or indirectly linked to a supplier through directorships held, joint addresses or telephone calls made. Intricate relationships are especially difficult to comprehend without graphical representation.

Information on hidden relationships can be obtained from:

- sender fax numbers on seized faxed documentation;
- business cards found on the premises;
- e-mails;
- records of telephone calls made internally, downloaded from the PABX system or cellphone records obtained from the service providers, and
- information searches on external databases such as ITC, Kreditinform, Experian and the Registrar of Companies.

i2's Analyst's Notebook is a package used with great success by organisations such as the FBI, Europol and the Scorpions. This software graphically portrays relationships between elements, chronologically analyses events and creates transaction flow charts. Integrated with Analyst's Notebook, i2 has also developed PatternTracer to aid with the identification of patterns within data.

The i2 range of software's broad application possibilities are demonstrated by it being instrumental in both the tracing of the origins of the ILOVEYOU computer

virus and identifying the cause of the Concorde crash. The strategic partnership between i2 and LexisNexis™, a global provider of online public information, could have a tremendous impact on forensic investigators, especially if South African databases follow suit.

Case management systems for successful investigations

It is a challenge to manage a large team of investigators and to ensure that nothing falls through the cracks. Team members may be geographically spread out and include people from various disciplines including accountants, lawyers, computer experts and psychologists.

Computerised case management systems facilitate the management of the investigation from its inception, through documenting the scenarios and allocating time, budgets and resources, to finalisation of the report and the creation of charge sheets.

A pre-programmed evidence matrix, incorporated in a system such as GEMS, is a huge advantage. Evidence matrixes assist with the breakdown of allegations into individual offences, and contain a list of the elements needed to substantiate a charge. GEMS ensures that an investigation is output driven and makes efficient use of limited resources.

Ideally a case management system should be able to handle a wide variety of document types, including charts, databases, scanned images, voice clips and analysis charts. The system should also preferably be able to search across different investigations and be accessible to remote users over a wide area network (WAN) or even the Internet.

Using the internet for fast 'fact' finding

During a forensic investigation, limited resources have to be focused on those areas with the highest potential 'rate of return'. This requires the ability to gather background information quickly and build profiles of the suspected companies and individuals.

The internet is probably the undisputed, quickest source of both national and international information. This information is literally available at your fingertips, and mostly for free!

The usually limited client information is normally used as a starting point to search through press articles and tap online databases such as ITC, Kreditinform and SAFPS. These online databases are usually available to subscribers for a minimal tariff per individual search.

It is, however, of utmost importance that the investigators remain aware of the restrictions on the credibility and accuracy of information posted on the Internet. Every scrap of information obtained through the Internet has to be substantiated, with additional evidence, such a property title documents and testimony, confirming connections between individuals.

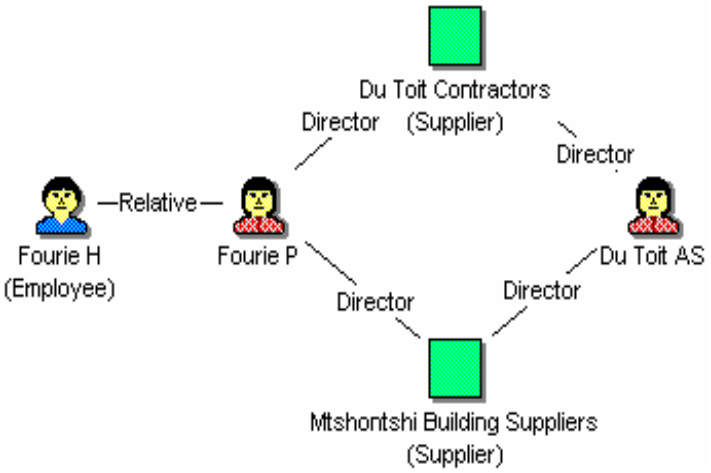
It takes skill and experience, not only to *find* the necessary information, but also to determine which information should be used and which discarded. Searching for 'John Smith' on the Internet will probably lead to a tangled web of misinformation. This could easily send the unwary investigator on a wild goose chase, quite the opposite of what he set out to achieve.

Clearer reporting

When all the cloak-and-dagger business is over, not to mention the endless hours of painstaking research and analysis, what remains is to summarise the investigation into a detailed report.

Surprisingly, this 'summarisation' could easily take up to a third of the total time spent on the investigation!

A picture does indeed speak a thousand words, not only during the investigation, but especially when presenting the results to the court, client or disciplinary hearing. This is clearly illustrated by this relatively uncomplicated chart created using Analyst's Notebook. The chart shows an employee linked to a supplier of the company. In addition, this supplier makes use of 'affirmative action window dressing'.



One of the most difficult aspects of a voluminous report is certainly to organise and keep track of the exhibits. This is easier said than done. Here the electronic database of the documentary evidence prepared during the investigation stage can again be of great help. The key documents can more easily be located through a keyword search. An extract of the identified exhibits' original filing numbers and descriptions could become the exhibits list with minor modification. The final report's exhibit numbers are then added in an adjacent column to enable the court, defence and prosecution to refer to their imaged copies of the documents, where they are available.

The invaluable human element

Regardless of how much 'artificial intelligence' and how many sophisticated investigative tools are used, they remains just that – 'artificial' and 'tools'. There is just no substitute for the human mind, supported by proper training and experience. Technology can speed up the investigation process but is no substitute for "gut feel" and physical interaction with witnesses and evidence.