

# INVESTIGATIVE SKILLS FOR THE 1990S AND BEYOND

**David Thompson**  
**Detective Sergeant**  
**Fraud Squad (Computers)**  
**Victoria Police**

## **Computers: The New Criminal Modus Operandi**

COMPUTER CRIME, HIGH-TECH CRIME, AND COMPUTER FRAUD ARE ALL terms used to describe the involvement of computers in the commission of crime. Computers have become a common business and household item and come in the form of personal organisers, notebooks, laptops, desktops, networks, mini and mainframe computers. Computer technology has not introduced a new crime but has changed the form of traditional commercial-type crimes. Committing crimes by computer can be viewed as a new modus operandi in the commercial crime field. Crimes that were once committed with pen and paper are now often committed in a computer environment.

Due to the changing form of business information systems, investigators are experiencing a substantial increase in the amount of computerised information forming part of current investigations. This information ranges from complainants' computerised company records to the seizure of suspects' computers and computerised records.

Since 1980, the form of business information systems has changed substantially. Many organisations now operate some form of computerised information system ranging from word processing to entirely paperless trading (which involves only computerised transactions and documents).

## **Investigators' Skills**

No longer do commercial crime investigators only require an understanding of accounting and business practices to perform their job. They must also have an understanding of computer technology and business information systems in order to identify and gather evidence during investigations. It is now necessary for detectives to be computer literate enough to competently search and seize computerised information systems (particularly personal computers). Investigators also require

sufficient skills to analyse and identify information of evidentiary value from typical computerised business records.

### **Changes in Investigative Skills and Practices**

This changing form of commercial crime has highlighted some deficiencies in the existing investigative practices, skills and knowledge of investigators who are required to deal with crimes involving the latest business technology. The investigative skills and practices of the law enforcement community have changed little over the past few decades. Until the 1990s, little attention had been paid to the impact of computer technology on the nature of business information systems—particularly the impact that computer technology has had on the ability of detectives to search, seize and analyse documentary evidence.

The computerised document has had a significant impact on the investigator's ability to prove the identity of offenders who have used documents to commit crimes. No longer are fingerprints, handwriting, typewriter analysis (although limited printer analysis is possible), indentations or pen striations able to be used to provide a nexus between the criminal and documents used to commit crimes involving computers.

Many experienced investigators have limited computer literacy. In fact, some of these investigators believe that there is no need to improve or develop new skills because they have never required specialist technical knowledge in any other field in order to investigate crimes. The fallacy in this argument is that, for centuries documents have been recorded on paper, and now documents are being created and stored on computers—even to locate and read a document requires some computer knowledge. Greater knowledge is required to successfully preserve, search, seize and analyse typical computerised business records and systems.

In order to efficiently and effectively conduct investigations in the commercial environment, investigators' skills and knowledge must keep pace with the technological changes in the general business community. It is essential that law enforcement agencies recognise the need to keep abreast of these changes and implement strategies to develop new skills, knowledge and work practices related to current business technology. It is also essential that computer technology is used to aid investigation for two reasons: firstly, to support the processing of information related to an investigation; and secondly, to actually facilitate the conduct of an investigation in the computer environment.

### **Use of Computer Technology to Aid Investigation**

Due to the nature and complexity of commercial crimes, it is very time-consuming to record, store, retrieve and analyse information relating to investigations. It is in these tasks that the use of computers by investigators will provide more accurate and efficient handling of documents and information and a more cost effective use of equipment and resources. Some of the major functions for which computer technology can be used to support investigations are:

- case management systems for investigation and administrative data;
- preparation, storage and retrieval of briefs of evidence and other documents related to investigations;
- analytical and intelligence systems to support investigations;
- access to the police and other government agency on-line computer systems;
- access to other relevant external on-line computer systems;
- use of portable computers in the field; and
- use of application software to support investigations.

#### *Case management systems*

A computerised database of information relating to investigations should provide an ability to store and retrieve information relating to complainants, suspects, victims, witnesses, businesses, addresses and other relevant information. The information known by an investigator is of great importance to other personnel in both the administrative and investigative roles.

An efficient and effective case management system will not only provide important administrative information, it will also be an investigative aid by providing historical and current information about investigations, which are not easily identified or retrieved from manual information systems.

#### *Preparation of briefs of evidence*

The process of preparing and storing information relating to briefs of evidence should also be computerised. All statements, witness lists, exhibit lists, informations, spreadsheet charts, graphs and database records should be stored on computer for easy retrieval, amendment and compilation of briefs of evidence for prosecution. This procedure enables all relevant information on a particular investigation to be efficiently controlled and easily located by members requiring access.

Standardised forms such as witness lists, exhibit lists, informations for an offence and warrants can be created. This will enable word processor operators or data entry staff to produce standardised documents for briefs of evidence, and release detectives from the task of preparing their own proformas during an investigation. The ability of micro-computers to expedite time-consuming tasks performed by detectives (such as typing and collating) will now allow detectives to spend more time actually investigating.

#### *Intelligence and analytical systems*

Analysis of collected and stored information can be used to identify similarities in cases; this may identify suspects and offenders for offences with no known suspects. Offences can be analysed and grouped using details such as modus operandi, suspect or car descriptions to aid the apprehension of the offender.

Analysts can provide accurate and current information on known suspects, offenders, premises and vehicles to assist in the identification of offenders responsible

for unsolved offences. This is done by searching the profiles of known persons and identifying all the offences in which particular suspects or offenders were involved.

There is a need for an intelligence and analytical function to support investigation of complex crimes which typically involve numerous associations between persons, companies and business transactions. The preparation of link analysis charts and association matrices are valuable aids to investigators during complex investigations.

#### *Access to police and government on-line systems*

There is a need for access to police and other government agency computer systems. Investigators have had access to computerised information such as criminal records, motor vehicle and licence details for over a decade, which has proved to be a valuable resource during their investigations. It is now time to integrate local personal computing resources with other police and government systems. Access to these systems will enable investigators to use corporate and government data, which can be analysed locally, to assist investigations.

External computer systems operated by other government agencies—such as the Cash Transactions Reporting Agency (CTRA), the Australian Securities Commission (ASC) and the Titles Office—will be of substantial benefit to investigators in the task of tracing financial and other paper trails. The opportunity to access these systems is readily available, others may require negotiation with the appropriate government departments.

#### *Access to other external computer systems*

With the increasing availability of publicly-accessible on-line database systems, the opportunity for investigators to remotely access other external computer systems will also provide a valuable investigative resource.

#### *Portable computer facilities*

There is a need for access to portable computing facilities to support investigations conducted away from the office. The ability to type statements obtained from witnesses directly into a computer in the field will eliminate the double handling of handwritten statements which have to be typed on return to the office. Where numerous documents are required to be handled, a portable computer could be used by investigators to transport all the necessary information required to conduct their inquiries—such as a full copy of exhibits, statements, database information and other relevant files. Without the assistance of information stored on computer, detectives will very often be confined to the office when interviewing witnesses because it is not practical to transport all the documentary evidence to a witness' premises.

Communication from the field using a portable computer via modem access to the telephone network will enable access to the computer facilities of the investigator's office. This will save time as it will no longer be necessary to return to the office to obtain additional information required during an investigation. Modem access would enable communication with the office from local, country, interstate and overseas locations.

*Use of application software to support investigations*

Computers can be used as an aid to investigations by performing the following functions:

- the use of databases to record, collate, and analyse exhibits, financial transactions and other documents;
- production of spreadsheets of financial data relating to investigations;
- the use of text retrieval software to analyse textual information relating to investigations;
- production of graphical representations such as flow charts, graphs and other images as an investigative aid and for ultimate production in court;
- the use of optical scanning technology to reproduce image or textual documents for analysis or presentation at court;
- the use of geographical mapping software to map known locations of suspects or incidents;
- the use of hypertext software to allow the linking and analysis of information collected during an investigation, in a manner not bound by the structure of database systems; and
- the use of expert systems to provide a standardised manner to perform tasks requiring expert or specialist knowledge.

Database software: Due to the volume of information collected during a commercial crime investigation, it is a very difficult and time-consuming task to sort and collate documents for analysis and presentation at court. It is essential that any information and documents—such as cheques, invoices, and other financial or business records—are collated and analysed in differing sequences to identify items of evidentiary value and to determine what offences have been committed. The task of analysing and collating exhibits can often take many months, due to the cumbersome and repetitive nature of this task.

With the aid of computers this information can be input into a database and the analysis of this information can be completed in a much shorter time span. Although time must be spent entering information into the computer, this task could be undertaken by data entry staff. The benefit obtained by entering this type of information into a computer is that it may be resorted and queried many times with the results being available immediately. The computerisation of some investigations can save many months of repetitive manual sorting, resulting in the early apprehension of offenders.

Spreadsheets: A spreadsheet, or ledger sheet, is primarily used in business by accountants for performing financial calculations and recording transactions. An electronic spreadsheet is simply a computerised version of a traditional spreadsheet. Spreadsheets can be used to analyse financial or other numerical data collected during investigations. They can also be

used to view and analyse the computerised records of victims or suspects seized during an investigation.

Text retrieval software: Text retrieval software can be used to search and analyse existing word processed documents such as statements, exhibit or witness lists, intelligence reports, warrants and investigation logs which are created during the course of investigations. It can also be used to analyse paper documents which have been optically scanned (OCR) and stored as text files, or computerised text files seized or obtained on computer storage media during an investigation. The documents can be searched for specific words, phrases or similarities which can then be retrieved for viewing, copying and manipulation. The text of a document can be manipulated in a word processing environment and then exported for input into a database or spreadsheet for sorting, query or further analysis.

Graphic representation: Graphics software packages can be used for the production of graphs and charts, and the summarising of data for presentation purposes. They can be used for presentations on monitors or can be printed for distribution. The printed output from these packages can also be used to create slides or transparencies. These different forms of output could be used for briefings, analysis and to assist the presentation of evidence in court.

Graphical representation of financial transactions has proven to be an extremely useful aid during investigations and in presentation of complex transactions to the courts. This process can now be performed using computer graphics technology which is far more efficient than the previously hand-drawn charts. The cost savings and flexibility of altering computer-generated presentations during investigations or court hearings have been demonstrated in a number of recent cases.

It is now possible to use personal computer charting programs to create graphic charts. It would be of benefit to investigators to be able to use a computerised charting facility during investigations to depict financial information and other link analysis charts. This facility is an essential aid to the investigation of complex commercial crime matters which will replace the hand-drawn charts currently used. The charts drawn by the investigators could then be used as the basis for the final charts prepared for court presentation.

Optical scanning of documents: The time-consuming task of keying documents into a computer can be further expedited with the assistance of a digital scanner using image or optical character recognition (OCR), software which optically scans a document and stores a copy of it digitally. The documents can then be retrieved to enable viewing of graphical images such as cheques, or the searching or manipulation of textual data. This facility would be of value where numerous exhibits are scanned as images and appended to a database for sorting, analysis and viewing. The computerised image could then be shown to witnesses and reproduced for inclusion in briefs of evidence. Ultimately, optical scanning can be used as an aid in the presentation of exhibits to the court.

Hypertext software: Because the process of investigation is not an organised and structured process, the use of database management software to organise data collected during an investigation can be restrictive when trying to establish links and associations. The use of hypertext software to link and analyse information collected

during an investigation is a viable alternative, due to the fact that hypertext is not bound by the structure of typical database systems. Hypertext type software will generally allow the operator to make links and associations as required. This could be very useful for intelligence analysis and investigative functions.

Geographical mapping software: The task of collating and analysing the locations and geographical relationships between offences can be aided by the use of geographical mapping software. The locations of suspects or incidents can be entered or imported from other computer systems to allow geographical analysis and presentation by investigators.

Expert systems: There is an opportunity for the use of expert systems in the investigative function. These systems use 'deductive reasoning' which is the same process that investigators use to solve crimes. The prospect of using computers which are able to process information at much faster speeds than humans, and the ability to reference much larger databases of information, is likely to greatly enhance an investigator's ability to solve crimes. These systems could provide the skills and knowledge of the most experienced investigators in the entire organisation. What must be remembered is that an expert system will not replace investigators, but it will assist them to perform more effectively and consistently. Expert systems could be used to support investigations in the following areas:

- an investigator's notebook that tracks and maintains a log of all actions taken during an investigation, including all inferencing, evidential reasoning and 'what if' capabilities;
- on-line intelligent access to existing databases;

- assist in criminal profiling of offenders by identifying major personality and behavioural characteristics and analysing the crime scene and other related evidence; and
- link analysis to identify relationships between persons and then make deductions about other relationships in order to assist the investigation.

#### *Use of computer technology to conduct investigations*

As commercial crime offenders are known to often use the most advanced technology available to support their criminal activity, it is now necessary for investigators to use similar technology in their efforts to investigate this form of crime. Commercial crime investigators are currently finding computer facilities located at many of the premises being investigated. The evidence that is being sought is often located in a computer environment which requires the use of computer equipment and software to facilitate search, seizure and retrieval. If investigators are to be successful, they must not only understand the technology but must also have access to it as an investigative tool.

#### **Computers: The New Investigative Tool**

Investigators require access to computer hardware and software to assist in the conduct of investigations. The investigative computer functions can be broadly categorised as follows:

- search and seizure of computers and computer storage media;
- analysis of computer evidence; and
- interception and monitoring of data communications.

The recovery of data from computers is a new law enforcement speciality. Some law enforcement personnel consider it a new Forensic Science which requires knowledge of the laws of search and seizure, rules of evidence and extensive computer knowledge (Stites 1990).

#### *Search, seizure and analysis of computer systems*

Criminal investigations involving computers and related technology require hardware and software to support the search, seizure and analysis of evidence obtained. Evidence obtained cannot usually be viewed or analysed without the aid of computer hardware and software. In many cases the evidence obtained may be from a system that is not compatible with the standard police equipment used for analysis. Therefore, investigators require access to a variety of computer hardware and software (application and operating system) or equipment that will allow the conversion of information from different environments and types of computer storage media.

Many software packages—such as industry standard application software packages, audit utility software, virus detectors, operating systems, utility programs and decryption programs—are required by investigators to aid the search, seizure and analysis of computers and computer evidence seized. These software utilities are used to access, copy and analyse data seized or identify deleted or 'hidden' files used by

offenders to hide evidence from investigators. In many cases files which are 'hidden' or erased can be retrieved by using these special utilities. These packages also provide the facilities for a detailed analysis of the computer system configuration which is of importance to the investigator.

#### *Interception and monitoring of data communications*

Due to the fact that many offenders utilise telephones, computers, beeper messaging systems and facsimile machines to conduct their criminal activity, the use of equipment to intercept these communications will be extremely useful in associating suspects with transactions where there is no personal contact with victims or other involved parties. The sophisticated equipment to monitor and intercept these devices is currently available and is going to become essential as transactions continue to become computer and telecommunications-based.

Access to current technology is urgently required by investigators in this technologically-complex field. It is important to recognise that technology-related crime is based in a rapidly changing environment. The tools used to combat it must be continually evaluated and regularly upgraded to ensure that the most efficient and effective use of resources is achieved.

Whilst the use of computer technology will provide the means to identify and gather computer evidence, it is essential to develop policies and procedures to ensure consistency in investigative practices in order to preserve originality, continuity and admissibility of gathered computer evidence. These practices and guidelines can be presented to investigators through new training programs relevant to this field.

### **Development of Investigative Computer Skills and Practices**

#### *Computer application software training*

In order to effectively use computers to support investigations, investigators should at least understand the operation of personal computers and develop proficient skills in the use of application software, such as word processing, databases, spreadsheets and any other relevant packages. These skills will be a sound base for the development of the computer investigative skills required to use the computer to conduct investigations involving the search, seizure and analysis of computers and computer evidence. Before attempting to develop computer investigative skills, investigators should have gained some initial computer literacy. This can be gained from a training program on the introduction to personal computer operations and application software use.

*Investigative computer training*

The computer training of investigators should be based on the nature of offences they will be expected to investigate. The nature of the offences are best categorised by the degree of technical expertise that may be used by offenders to commit computer-related crimes. The nature of computer crime can be classified into three basic technological categories (identified by Federal Bureau of Investigation research in the USA):

- computer operations (input, output);
- programs and data (processing); and
- systems and communications (environment and transmission).

A training program for investigators in this field should separately address the degrees of technical skill with separate levels of training. The training program should only attempt to address the first two categories of technical expertise because the third category is an extremely technologically-complex domain which should be left to specialist computer professionals (who can be utilised as consulting experts).

*Training program structure*

The skills required can best be provided by a three-tiered training program which is provided to detectives in progressive phases, based on their specific investigative function.

- Level 1 — Awareness Skills (theoretical): this level is not related to the technology categories, but is a prerequisite for Level 2 training;
- Level 2 — Broad Knowledge (theoretical and practical): to address the skills required for investigations involving computer operations (input, output) (Technology Category 1); and
- Level 3 — Sound Knowledge (theoretical and practical): to address the skills required for investigations involving program and data manipulation (Technology Category 2).

The training program should provide the opportunity to present the skills required by the generalist investigator through to the specialist computer crime investigator. All investigators should at least have a theoretical awareness (Level 1) of the technological issues that apply to an investigation in the computer environment. Detectives assigned to specialist commercial crime duties (such as the Fraud Squad) should have a broad understanding of computer technology issues (Level 2), with theoretical and practical expertise in the personal computer environment. Specialist computer crime investigators should have a sound understanding of computer technology (Level 3) to enable them to undertake complex technological investigations in all environments (with or without consultant experts).

It is not suggested that all investigators require an extensive knowledge of computers (although this may be the case in the future), merely a sound understanding

of computing principles and practices in relation to small computer systems (personal computers) used by most businesses today.

*Specialist computer training*

Whilst the three-tiered training program should cater for most skills and knowledge required by investigators at different levels, there will be occasions when additional skills and knowledge will be required by investigators, particularly those who have completed the full training program. Provision should be made for ongoing training of the members involved in the specialist investigative computer analysis function to ensure that their knowledge and skills are maintained.

The nature and extent of training in this field will become an important factor in determining whether the law enforcement community will have the capacity to efficiently and effectively investigate modern commercial crime.

*Research and development of computer investigative techniques*

Although the methodology for the investigation of technological crime is based on general investigative procedures, the technological components require a renewed approach involving the development of new techniques and use of new equipment. In 1991, the law enforcement community in Australia does not have access to advanced techniques to aid in the retrieval, seizure or analysis of computer evidence.

A number of investigative procedures and techniques for search, seizure and analysis of evidence in the computer environment using standard industry tools have been developed. Yet there is a need for more advanced techniques to be identified and used to support investigations involving the analysis of evidence from computer environments. Some of the areas which need to be addressed are :

- the conversion of computerised evidentiary information from differing storage media and formats to a form which is compatible with the systems being used by investigators for analysis;
- the analysis and comparison of electronic and computer printed documents to determine characteristics of an evidentiary value;
- the analysis and retrieval of data or programs which have been deleted, changed, hidden or encrypted on computer storage media; and
- the development of specialist computer software utilities to aid the search, seizure and analysis of computer systems and data.

## **A Example of a Computer Training Program**

The Victoria Police Fraud Squad conducts a three-tiered computer training program which is consistent with the model discussed. The three levels of training are provided to detectives in progressive phases which provide the knowledge and skills required for their specific investigative function. The computer training program consists of the following three levels:

- Economic Crime Course, computer segment (theoretical);
- Business Systems for Investigators Course held at the Royal Melbourne Institute of Technology (RMIT) (theoretical and practical); and
- National Computer Crime Investigators Course, held annually (theoretical and practical).

### *Economic Crime Course, computer segment*

The Fraud Squad Economic Crime Course (general training course) currently provides theoretical instruction on the investigation of crimes in the computer environment as part of the syllabus (equivalent to Level 1 training). This segment is aimed at new members of the Fraud Squad or those with limited fraud investigative experience. This component broadly covers the following topics:

- introduction to computer technology and terminology;
- legislation related to crimes involving computers;
- evidentiary legislation and issues; and
- investigative procedures and practices.

### *Business Systems for Investigators Course*

This advanced training course has been implemented to provide the skills necessary to bridge the gap between the Economic Crime Course and the current National Computer Crime Investigators Course. This course provides the knowledge and expertise required to search and seize a personal computer in order to gather computer evidence. The course aims to provide the following skills and knowledge to participants:

- familiarity with the major features of computer systems sufficient to determine the difference between small and large computer systems;
- the ability to recognise and use the basic features of generic computer software packages used by businesses;
- the ability to identify and recognise software package-related characteristics of files and data used on personal computers;

- the ability to identify and recover computerised data stored on a personal computer which is required as evidence, without damage;
- familiarity with the basic terminology, tools and procedures used to examine computers and computer storage media; and
- practice in the investigation of small computer systems using standard tools and investigative procedures for identifying and gathering computerised information.

This structure is similar to a typical tertiary subject presentation and is considered the best approach to ensure maximum comprehension and retention of the information and skills presented. The duration, course content and method of assessment is consistent with the subjects taught in other business computing courses at tertiary level.

The content of the training course satisfies the prerequisite level of training required for the National Computer Crime Investigators Course. This will provide a pool of investigators from which to annually select members who are suitable to go on to more advanced computer crime training.

#### *National Computer Crime Investigators Course*

The National Computer Crime Investigators Course aims to provide a sound knowledge of computer technology and the investigative techniques and procedures required to investigate complex crimes in the computer environment. The objectives of the course are to:

- provide an overview and definition of crimes in the computer environment;
- provide knowledge of the current and emerging technologies, procedures and practices being used by the business community in the computer environment;
- provide a knowledge of the investigative techniques, procedures and practical skills required to investigate complex crimes in the computer environment; and
- provide a knowledge and understanding of the law and prosecution procedures related to crimes in the computer environment.

#### **The Future**

According to law enforcement futurists, as law enforcement focuses its attention on the traditional crimes (those with which it understands and is equipped to deal with) computer crime is emerging as a threat to the economy and national security. What may be portrayed as a sudden and dramatic increase in high technology crime has grown steadily for a decade and largely been ignored (Tafoya 1987). It is predicted that the law enforcement community could be overwhelmed by technologically-sophisticated crime and may be reduced to taking preliminary reports while the

investigations are conducted by private organisations of contracted specialists (Temby & McElwaine 1987).

The failure of the law enforcement community to recognise the problems and provide adequate technical skills and facilities for investigators may have a substantial effect on our ability to deal with this form of crime. The law enforcement community must recognise the problem and understand the techniques and technology that may be employed. If investigators fail to provide an appropriate and effective response to crimes involving technology, they will be compelled to endure the future by failing to shape its course (Tafoya 1987).

The important issue to be recognised in relation to computer crimes is that they are coming to notice more often. The law enforcement community must prepare itself to deal with the investigation of commercial crime which will soon be extensively computer-based. In a report to the USA Congress in 1990, William Sessions, the Director of the USA Federal Bureau of Investigation stated that:

in the continuing fight against computer crime, the law enforcement community must continue to strengthen its investigations, training and support services (Sessions 1991, p. 13).

A failure to address these issues may confirm the futurists' predictions.

## References

Sessions, W.S. 1991, 'Computer Crimes: an escalating crime trend', *FBI Law Enforcement Bulletin*, vol. 60, no. 2, February, pp. 12–15.

Stites, C.M. 1990, 'PCs—Personal Computers or Partners in Crime?', *Law and Order*, vol. 38, no. 9, September, pp. 161–65.

Tafoya, W.L. 1987, 'Into the Future . . . a Look at the 21st Century', *Law Enforcement Technology*, September/October.

Temby, I. & McElwaine, S. 1987, 'Technocrime—An Australian Overview', *Criminal Law Journal*, vol. 11, no. 5, October, pp. 245–58.