Goodbye Columbo, hallo cyber cops...

By Barry Bateman

As the world modernises and technology seeps into every facet of life, gone are the days of Columbo chasing a paper trail.

Instead it is the likes of Gil Grissom and his CSI team scouring the cyber world for clues. But the lights, camera, action style of Hollywood investigation is a far cry from the real world.

In South Africa top computer specialists are still working on procedures to collect digital evidence, because as in collecting biological evidence, it requires a sound procedure to be presented in and accepted by courts.

Council for Scientific and Industrial Research cyber security researcher Marthie Lessing has almost completed her doctorate in live forensics acquisition.

"Acquisition is getting the crime-related digital information from a computer or network.

"It is the most important part because if you do something wrong in that process, you cannot use it in court," she said.

Cyber crime was any unlawful act involving a computer, either as a tool in committing the crime, the target in the crime or both, Lessing said.

"This involves crimes such as hacking, ID theft and the dissemination of Trojan horses or viruses."

The head of the CSIR Safety and Security Competency Area, Dr Barend Taute, said that about 10 years ago the council considered what could be done about crime in South Africa.

They established a Crime Prevention Centre which eventually became the Safety & Security Competency Area within the operating unit Defence, Peace, Safety and Security. The Safety & Security Competency Area was divided into two research groups, focusing respectively on crime prevention and safety & security technology.

The latter group is divided into technology strategy and cyber security. "Research into cyber forensics started with support to law enforcement agencies.

"They needed to work at crime scenes where digital evidence needed to be recovered.

"We supported (the agencies) with training in application of a crime scene methodology and the analysis of digital evidence acquired at the crime scene," Taute said.

Lessing said the process of forensically sound, live acquisition was still being developed. "Our intention is to get this accepted in courts."

She said digital evidence is in some ways like biological evidence. "If an investigator collects biological samples without using gloves, he will contaminate it and it won't be accepted in court.

"Similarly, digital evidence needs to be collected using the correct process to enable acceptance in court," she said.

Taute said that when an investigator arrived at a crime scene and found a computer, cellphone or a digital storage medium such as a memory stick, they needed to know how to collect the evidence in a sound way that would stand up in court.

He said there were two problems when submitting evidence from a computer in court. "Firstly, digital evidence can be a technologically complex issue, requiring expert witnesses and familiarity with the terminology in court.

"Secondly, there is the issue of acceptance. Digital evidence is a recent development that has not been fully tested in court.

"A feature of digital evidence is that it is difficult to 'prove' that the evidence is original, unmodified evidence.

"This requires a sound evidence-gathering process, because opposing counsel will try to prove that the acquisition process was faulty," he said.

Taute said they were moving in the right direction, but as is common with technology it is constantly changing and provides new challenges for researchers trying to get a step ahead of criminals.

CSI: Top television drama

CSI: Crime Scene Investigation is an American crime drama television series that trails the investigations of a team of Las Vegas forensic scientists as they unveil the circumstances behind mysterious deaths and other crimes.

The show was created by Anthony E Zuiker and produced by Jerry Bruckheimer Television and CBS
Productions; now CBS Paramount Television. The ninth series, which sees the departure of William Petersen and
the introduction of Laurence Fishburne, will be shown in the US in October.CSI is syndicated across the world, including in South Africa.

The difference between dead and alive

Council for Scientific and Industrial Research cyber security researcher Marthie Lessing explains in her doctoral paper the difference between "dead" and "live" forensics. Dead Forensics Referred to as the traditional digital method, dead acquisition involves examiners pulling the plug on a suspect system.

This method avoids any malicious process from running on the system, potentially deleting data from the system. It gives the examiner access to a snapshot of the swap files and other system information as it was last running.

The formal definition is "... analysis done on a computer system that is powered off". This analysis is normally done by opening the computer machine box and removing the hard drive from the system. The hard drive then gets connected to a secure write blocker and the data acquisition can start.

Live Forensics It is similar to dead forensics, except that the suspect machine is still running. The machine is still live,with some processes running in the background. It developed in response to shortcomings of the dead forensic acquisition techniques, considering the retention of volatile data, and a countermeasure for encrypted files on a live system.

With live forensics, the investigator needs to do a bit-bybit copy of the machine's hard drive, without actually removing the hard drive from the machine.

Published on the web by Pretoria News on August 26, 2008.