

Top forensic expert puts CSIR on cyber map

With researchers like Pontjho Mokhonoana of CSIR Defence, Peace, Safety and Security, the wheels of justice are set to grind faster in the near future.

The 22 year-old is the only Encase certified forensic researcher at the CSIR and currently works in the safety and security research group.

Mokhonoana says EnCase is software used to analyse and examine data. "Simplified, it signifies that you have the theoretical and practical skills to perform computer forensic investigations," says Mokhonoana. Computer forensic investigations help to answer questions relating to the who, when and how a computer-related crime has been committed.



Pontjho Mokhonoana of CSIR Defence, Peace, Safety and Security

EnCase enables investigators to, among other things, acquire data in a forensically sound manner, using software with an unparalleled record in courts worldwide and investigate and analyse multiple platforms, including Windows, Linux, AIX, OS X and Solaris, using a single tool. Most importantly, it enables the investigator to find information despite efforts to hide, cloak or delete it, while also making it easy to manage large volumes of computer evidence, viewing all relevant files, including deleted files and other places on the drive that the operating system hides.

"Nowadays, more and more computers are being used, which means more crime is committed using computers," he says, adding that computer forensics helps the justice system.

If a cell phone, for instance, is used to record a video of criminal activity, the footage can be a valuable source of evidence and will need to be handled with proper care to ensure that it will stand in court. It is therefore important that the computer investigator is skilled and follows correct procedure.

The certification recognises that an investigator is a skilled computer examiner with at least 18 months of investigative experience. When asked how he feels about obtaining the certification, he says: "To complete the practical part of the certification was a mammoth task; it could only be done by working very long hours. I suppose the fact that I am one of only a few Encase certified computer forensic investigators in South Africa implies that this is an achievement."

Mokhonoana has a BSc Honours in computer science from the University of Pretoria and is currently reading towards his Master's degree.