Fighting cyber crime through cyber forensics first responder training

JP VENTER, S NARE
CSIR Defence, Peace, Safety and Security, PO Box 395, Pretoria, 0001, South Africa
Email: jpventer@csir.co.za – www.csir.co.za

INTRODUCTION

The rapid development and use of information and communications technology (ICT) has influenced everyday life, mostly in a positive manner. This technology is, however, also available to the criminally minded. Activities performed through ICT leave behind traces that are of interest to cyber forensic scientists. Cyber forensics is the science of analysing these traces in order to extract evidence for use in court or at formal hearings. This rapid rise in the use of ICT for criminal purposes necessitated the further development and expansion of cyber forensic expertise (Rogers 2004).

Training in this environment is complicated due to the lack of sufficient human resources with a background or formal training in ICT. A further complicating factor is that individuals formally skilled in any form of ICT are difficult to retain within the criminal justice system. Existing human resources, even when not formally skilled in ICT, must be utilised in the cyber forensics environment.

OBJECTIVES

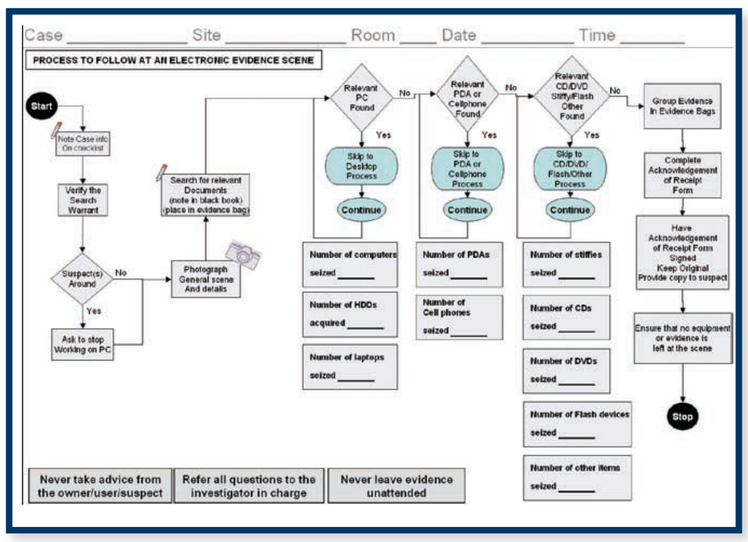
The first person to secure the electronic evidence on a potential crime scene is called a 'cyber first responder'. It is vital that the cyber first responder understand and follow the correct procedure in searching for and collecting (search and seizure) and duplicating (acquisition) the electronic data that may contain evidence. The objective was to develop a course customised to the South African environment to develop the skills of cyber first responders.

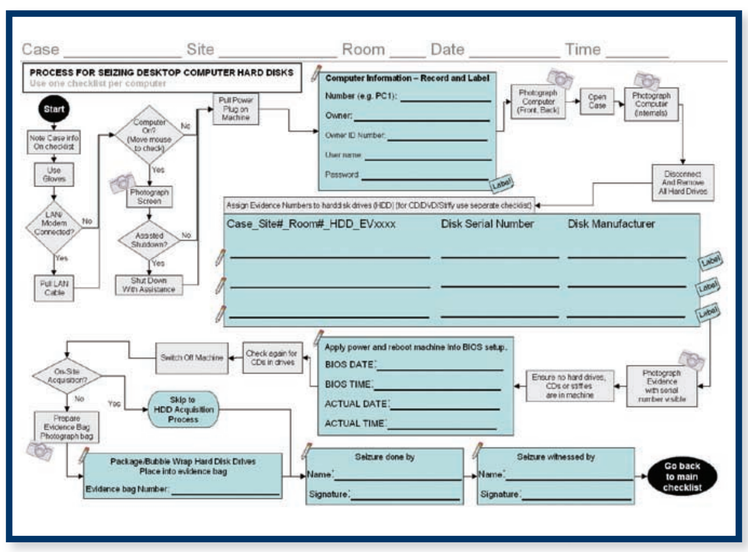
The specific outcomes for the course were to enable cyber first responders to:

- Explain the essence of cyber forensics
- Apply processes involved in cyber forensics first response
- Acquire and copy digital data at basic level
- Facilitate the search for and seizure of electronic evidence
- Generate and utilise documentary aids before and during the computer-related crime investigation.

COURSE LAYOUT

The course started by providing the participants with an overview of the cyber forensic process as indicated in Figure 1. The rest of the course covered areas such as: The law, the chain of custody, search and seizure, acquisition, documentation and discipline.





The course made use of the CSIR-developed process flows. These process flows enables non-ICT professionals to follow a well-defined and easily-documented process (Venter 2006). Examples of the process flows are shown in Figures 2 and 3. The process flows enable the cyber first responder to work approximately 25% faster and make fewer mistakes.

The course includes a rigorous practical aspect. A crime scene is created and each learner must follow the process taught in the course to handle the scene. Each learner is evaluated by a facilitator and feedback is provided at the end of the course. This ensures that the individuals successfully completing the course will immediately be confident enough to apply the techniques learned in real investigations.

CONCLUSIONS

More than sixty learners have already successfully completed the course. The result of the training is a criminal justice environment better equipped to handle the growing volume of cyber forensic activities. The research performed by the CSIR provided internationally-recognised enhancements and greatly reduced the training effort while at the same time improving the cyber forensic operational effectiveness.

Cyber criminals use modern technologies to con unsuspecting users – holding the world to ransom. CSIR researchers investigate ways to combat the scourge of computer-aided crimes.

REFERENCES

1. Rogers, M. K., The future of computer forensics: a needs analysis survey, Computers and Security, Volume 23, Issue 1, Elsevier, February 2004.
2. Venter, JP. 2006. Process flows for cyber forensic training and operations. 2nd Annual IFIP WG 11.9 International Conference on Digital Forensics, Orlando, USA, 2006, 21p