Process Flows for Cyber Forensics Training and Operations

J.P. Venter

CSIR Defencetek

Meiring Naude Road

Pretoria, South Africa

Email: jpventer@csir.co.za

Telephone: +27 12 841 2011

Fax: +27 12 841 2528

***Abstract-* The demand for Cyber Forensics capabilities is growing rapidly. This places stress on the development of human resources that can cope with the requirements of Cyber Forensics. Suitable candidates with enough technical background, training or insight are not always available or retainable. The training of Cyber First Responders is therefore a challenge. Current material is mostly in the form of unstructured lists and requires a certain amount of understanding of the technical field from first responders, which they may not have, in order to make decisions as to what exactly to do at a cyber crime scene. In this paper the development and testing of Cyber First Responder Process Flows is discussed. A generic process flow framework is presented and design principles and layout characteristics as well as important points within the process flows are discussed. The positive impact of the process flows during cyber forensic first responder training is then indicated. The hypotheses that the process flows will speed up a cyber forensic investigation, even for experienced cyber forensic investigators, was tested and confirmed. The use of the process flows during Cyber Forensics operations is indicated. The paper concludes that the process flows was shown to be beneficial to first**

responders performing cyber forensic search and seizures, indicates that future work regarding enhancement and customisation of the process flows may be required, and suggest the use of the process flows in electronic format coupled to a case management system.

Keywords: Cyber Forensics, Process Flows, Training

I. Introduction

The rapid development and use of information and communications technology has influenced everyday life, mostly in a positive manner. The technology is, however, also available to the criminally minded. A study performed by the UK National High Tech Crime Unit indicates that the monetary impact of high tech crime was estimated at more than £2 billion for 2004 [4]. This rapid rise in the use of information and communications technology for criminal purposes caused the requirement for Cyber Forensic expertise to expand. In order to respond to a requirement to expand the Cyber Forensics capability within a certain section of the South African government, training in Cyber Forensics was required. The training in this environment is complicated due to the lack of sufficient resources with a background or formal training in information and communication technology (ICT). This is also true internationally as indicated by a recent study that found that only a small number of investigative units nationally (USA) have a computer scientist or other technically trained individuals on staff [3]. A further complicating factor is that individuals formally skilled in any form of ICT are difficult to retain within the criminal justice system. Existing skills, even when not in ICT, are therefore needed to be utilised in the cyber forensics environment.

The requirement was for more than just training focussed on the use of existing tools, such training assumed a certain level of understanding regarding an electronic crime scene; such training also assumes a certain level of understanding regarding computer and electronic systems. For the candidates to be trained this was not necessarily the case. Some of the candidates had only very limited understanding of computer and electronic systems. Most of the candidates had a good understanding of investigative processes however. Generally available information on the handling of electronic crime scenes is in the form of descriptions or lists (e.g. [2],[6],[7]). Most of the literature provides general principles; this is necessary but not sufficient to support the Cyber First Responders more detailed guidance is required. In some steps are provided but assumes ICT knowledge in understanding the impact or outcomes. For example [2] indicates one of the steps as: "For each system, obtain the relevant order of volatility". This assumes that the Cyber First Responders know the volatility of a system and can prioritise amongst others. Observing the students in the training setup this was definitely not the situation as some of the students would spend an inordinate amount of time on CDs and then had to rush through the process of seizing the hard disks, which are much more important, and in the process would make mistakes. In [6] much more detailed and sequenced information is provided. This information is however spread over several pages. It was observed that the Cyber First Responders did not refer back to this sort of information during the seizure or got the information mixed up because of it being distributed over several pages. This again caused anxiousness that led to mistakes being made. These lists based approach did therefore not provide sufficient support to the candidates.

To alleviate some of the problems mentioned earlier the Cyber Forensics Investigation process flows was developed. The purpose of the process flows was to ease the understanding and implementation of electronic crime scene search and seizure practices especially for individuals without a formal qualification in ICT.

The problem addressed in this paper is therefore how to support cyber forensics first responders, who are not IT professionals, during training and operations. The method used was to develop a model of the tasks that the cyber first responder needed to do. This was then packaged in terms of the process flows. The next step was to test the model. The model was developed during the first two training courses provided and then tested during the last two training courses.

This paper is organised as follows: In Section II background regarding the problem of training First Responders without an ICT background is stated, Section III provides detail regarding the design and layout characteristics of the process flows thought to be necessary to address aspects of the problem (a sort of a requirements specification), Section IV provides a generic process flow framework and discuss the various process flows (can be seen as the design and implementation section). In Section V the impact of the process flows, and the way that it addressed the problem statement, in the training context, is shown (a form of verification and validation). Section VI provides conclusions and indicates potential future work.

II. Background

Building the skills of cyber forensic experts is one of the areas that requires ongoing attention. A National needs assessment regarding law enforcement tools and technologies for investigating cyber attacks was performed by the Institute for Security Technology Studies at Dartmouth College in 2001/2 [3]. In this study participants indicated that training programs that fit law enforcement needs were a specific requirement. A study done by Rogers and Seigfried [5] published in 2004 supported this by indicating that education/training and certification was the most reported issue. This viewpoint was also expressed by a special investigation unit within the South African law enforcement environment.

Within the South African context the initial requirement was the development of individuals that could assist at electronic crime scenes and specifically with the collection of electronic evidence. The group of people responsible for this task is identified as Cyber First Responders. The primary responsibility of Cyber First Responders is to secure an electronic crime scene, search for devices containing any potential electronic evidence, and seizing such devices in a manner that will conserve the chain of evidence.

First responders need to understand the basic actions to take on an electronic crime scene. In support of this a large amount of information supporting cyber forensics is available. A good example of this is the US NIJ guide for first responders [6]. This guide provides excellent information applicable to the handling of an electronic crime scene. It however lacks the detailed information required by a first responder in the context of limited formal ICT training mentioned earlier. In order to address this gap the Cyber Forensics Process Flows was developed. The process flows provide a structured path of actions to follow and a means for first responders to check off the actions as they are taken. It was proposed that the flow diagram approach would be easier to follow confidently for less technically proficient persons than a list approach.

Beebe and Clark [1] argues that digital investigation frameworks should not use a checklist approach as each situation is likely to be unique and that different steps are likely to be taken in each situation The process flows can be seen as checklist orientated and will therefore be subject to critique. We argue however that the target audience of the process flows requires a more rigorous approach that will deal adequately with most situations. The argument is supported by [2] indicating that the amount of decision making needed to be made during the collection process must be minimised. It is further supported by [11] stating that following the process will lessen the chance of making errors and will facilitate good documentation. Individuals without a suitable ICT technical qualification or background should not take different steps because they may not be able to explain the implications thereof if challenged during testimony. It is further argued that the process flows adds sequence to actions in a manner that is easier to understand than the list approach. It is agreed that the objectives-based structure of Beebe and Clark [1] is more suitable to complex situations or more advanced phases of the overall forensic process. The focus of the process flows are on the handling of electronic evidence that does not involve complex set ups or complex environments.

The following hypothesis was formed at the start of the process flow development: Process flows will speed up a cyber forensic investigation, even for experienced cyber forensic investigators. This hypothesis was tested during the implementation of the process flows.

III. Process Flow Design Principles and Layout Characteristics

In this section we discuss the design principles and layout characteristics for the process flows. The actual process flows is discussed in the next section.

The first design principle was to ensure ease of use for non-IT professionals. As indicated in the problem statement a large number of the people available to perform Cyber First Responder duties are not ICT professionals. The Institute for Security Technology Studies survey [3] indicated that only 11% of their respondents had completed a full course of computer study in a computer related field. This percentage is likely to be even lower in the South African context. Cyber Forensics is however a technical computer related field. Adhering to the first design principle may then seem impossible to achieve though, as will become apparent later, it was possible to achieve. The cyber forensics field is very technical and do ask challenging questions, even to IT professionals. The focus of the process flows however is to develop a process that will enable **non ICT professionals** to perform adequately in the majority of cases.

This leads to the second design principle that required the process flows to be applicable in the most likely cases. A diverse set of equipment and installations of such equipment is found in the ICT environment. Developing process flows that will be able to deal with all these diversities would not be feasible. The cases that the process flows can deal with are therefore built around scenarios that occur most of the time. The most likely scenarios is based on the knowledge gained during involvement with more than 50 cases.

The third, and next, design principle required the process flows to, at least, not interfere with expert testimony and, if possible, actually assist with expert testimony. Investigators that have to present evidence are the most likely to appear in court. If a proper process was followed it should not be necessary for Cyber First Responders to appear in court. The process flows must take into account potential challenges of the evidence due to activities performed by the first responders. It is in this context that the checklist nature of the process flows may be challenged especially if it is not strictly followed and the expert witness cannot explain why the process was deviated from. We argue that given the target users of the process flows it is more important to ensure that a Cyber First Responder is confident when testifying to the process that was followed than the ability to handle exceptions. As indicated by Wolfe [8] a good attorney may be able to rattle or confuse a witness and by doing so can sometimes reduce or negate their testimony. Wolfe also indicates in [9] that close attention must be paid to strictly following and documenting the methodology used in the forensic process. The process flows support this by providing a well documented seizure process flow. The aim of the process flows is to assist the Cyber First Responder to report on the actions taken, with confidence.

The fourth, and last, design principle was that the process flows must be such that it can be utilised during operations and not only during training. Although the process flows originated in the training environment the knowledge gained by the participants must also be applied during operations and the process flows must support this. During the training sessions the participants indicated that they would definitely use the process flows in operations. It is therefore essential that the design is such that it will facilitate operational use.

The next aspect to consider is the layout characteristics of the process flows. Apart from the overall design principles certain layout characteristics of the process flows are worth mentioning. Although some of these characteristics may seem trivial they were only found to be important after the process flows were used in practice. The first characteristic is that each flow must fit on a single A4 page. The A4 layout allows for the use of the process flows together with a normal A4 record book. It also eases the duplication of the process flows for future use. The layout is also such that the process flows can be reproduced in black-and-white.

Recording information is vital throughout the forensics process, also during evidence collection [2]. The process flows support this aspects by ensuring that important information is captured whilst following the process flow steps. This ensures that the information is recorded and not forgotten. Information about a specific piece of evidence, for example a desktop computer, is kept together in one place. All information recorded is clearly associated with a specific case, site and room as this is also recorded on the process flows.

Certain naming conventions are indicated on the process flows. This reminds the first responders of the correct naming convention for a specific piece of evidence. For example on the process flow “PROCESS FOR SEIZING CD/DVD/STIFFY/FLASH/ OTHER” the naming convention Case_Site#_Room#_xxxx_EVxxx is shown. For the first xxxx part the descriptor to be added is then indicated as “CD/DVD/STIFFY/FLASH/OTHER”. In the applicable South African context this naming convention is used throughout the cyber forensics process and eases the task of the analysts as the origin of any evidence material is easy to trace.

IV. Process Flows

The initial set of process flows included one process flow to govern general behaviour on an electronic crime scene and three process flows dealing with specific device types. The generic framework elements present in all of the process flows is discussed first, other general aspects relevant to all the process flows is discussed second and thereafter elements of the specific process flows. Describing each step in each of the process flows is beyond the scope of this article.

The generic framework layout present in each of the process flows is shown in Figure 1. In each of the process flows an “Inspect & Prepare Scene”, “Collect Evidence & Evidence Information”, and “Debrief Scene & Record Seizure Information” element is present.

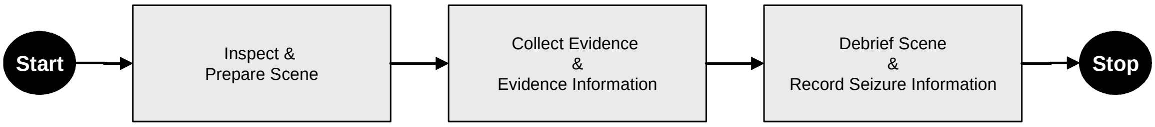

Start
Inspect & Prepare Scene
Collect Evidence & Evidence Information
Debrief Scene & Record Seizure Information
Stop

Figure 1: Generic Framework Elements

The “Inspect & Prepare Scene” element contain actions to prepare the Cyber First Responder for the tasks to follow (e.g.”Use Gloves” in figures 3,4, and 5), actions to survey the scene in general (e.g. “Suspect Around?” in figure 2), actions specific to the equipment to be seized (e.g. “LAN/Modem Connected” in figure 3), and actions to prepare the scene for the actual collection of the evidence (e.g. “Write Protect Stiffy” in figure 5).

The actions in the “Collect Evidence & Evidence Information” elements resolve around the recording of information related to the specific evidence aspects being dealt with (e.g. “Computer Information – Record and Label” in figure 3), assigning unique identification to each piece of evidence (e.g. “Assign evidence number, place in evidence bag” in figure 5), and noting special information (e.g. Apply power and reboot machine into BIOS setup” in figure 3).

In the “Debrief Scene & Record Seizure Information” element actions occur to record the existence/handing over of evidence (e.g. “Complete Acknowledgement of Receipt Form” in figure 2), collect evidence in groups (e.g. “Package/Bubble Wrap Hard Disk Drives – Place into evidence bag” in figure 3), and record the people involved (e.g. “Seizure done by” and “Seizure Witnessed by” in figures 3,4 and 5).
These generic framework elements create a sense of comfort with the First Responders because the same basic steps are followed for the various sorts of evidence to be handled.

The first general aspect is the recording of information on the process flows. RFC3227 [2] indicates that the “where”, “when” and “by whom” the evidence was discovered and collected must be noted. This is covered in the process flows through two means. Firstly at the top of all the process flows the CASE, SITE, ROOM, DATE and TIME details are captured. Secondly information is captured within the process flows. See for example the noting of the details of the person performing the seizure, and the person witnessing the seizure in figures 2, 3, and 4.

The second general aspect is using cameras. Photos are useful and important as indicated in [6], [7], and [10]. In all the process flows photo points are shown with a 📷. Photos assist in documenting the exact set up of the evidence, the cabling, the devices in a desktop, the image on the screen, etc. Photos also help in solving disputes about the set up, if any such occur later on. It has been found that the owner of a seized computer would later argue that the components in the computer have been replaced by inferior items. A photo of the original set up will quickly resolve any such arguments.

The process flow used from the start at an electronic crime scene is shown in Figure 2. This process flow starts by verifying the search warrant. It must be verified that the warrant covers the applicable electronic devices searched for and seized by the first responders. Another important aspect is to separate any person from any computer as soon as possible [11], this is indicated as the next step in the flow. The rest of this process flow focus on the identification and recording of evidence found whilst directing first responders to the appropriate detailed process flow. The sequence, PC then PDA or cell phone, then CD/DVD, Stiffy/flash, other, can be seen as a form of prioritisation. Computer hard disks hold the most data and are therefore the most likely source of evidence. Next are PDAs and cell phones that may contain a lot of valuable contact information. The last is other storage devices. A few special reminders, such as “Never leave evidence unattended” are also shown on this process flow.

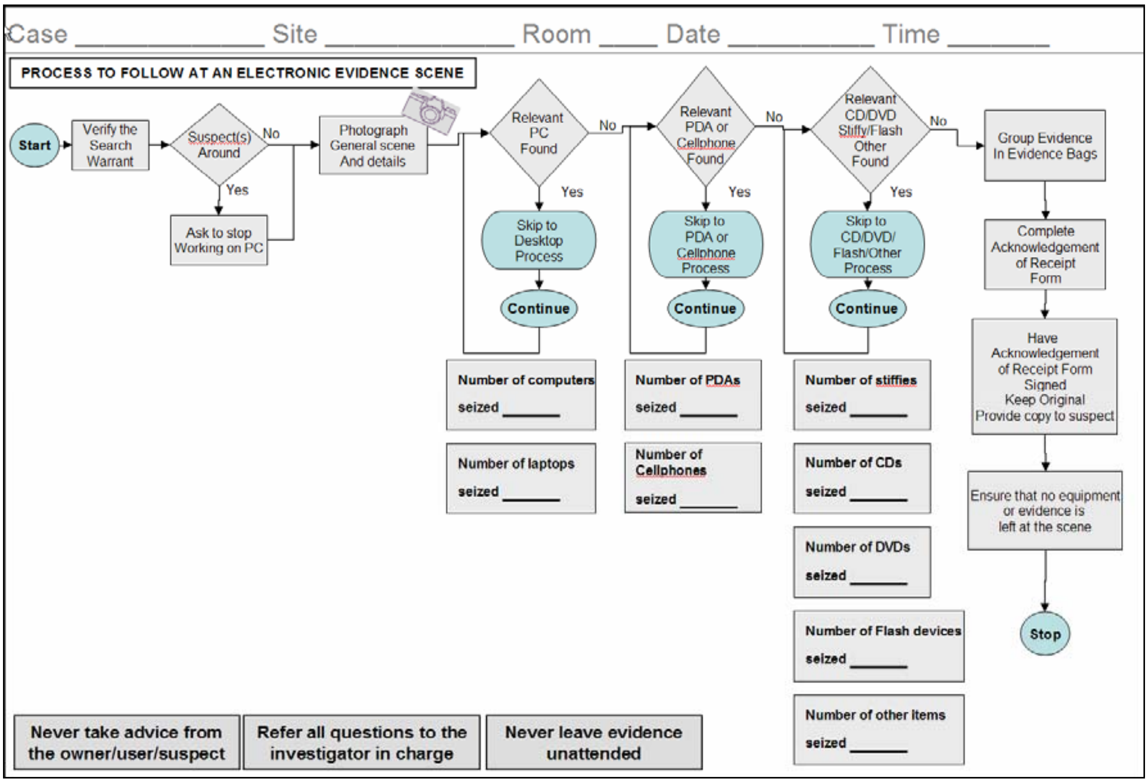

Case ____________ Site ____________ Room ____ Date __________ Time _______
PROCESS TO FOLLOW AT AN ELECTRONIC EVIDENCE SCENE
Start
Verify the Search Warrant
Suspect(s) Around
No
Yes
Ask to stop Working on PC
Photograph General scene And details
Relevant PC Found
No
Yes
Skip to Desktop Process
Continue
Relevant PDA or Cellphone Found
No
Yes
Skip to PDA or Cellphone Process
Continue
Relevant CD/DVD Stiffy/Flash Other Found
No
Yes
Skip to CD/DVD/ Flash/Other Process
Continue
Group Evidence In Evidence Bags
Complete Acknowledgement of Receipt Form
Have Acknowledgement of Receipt Form Signed Keep Original Provide copy to suspect
Ensure that no equipment or evidence is left at the scene
Stop
Number of computers seized ______
Number of laptops seized ______
Number of PDAs seized ______
Number of Cellphones seized ______
Number of stiffies seized ______
Number of CDs seized ______
Number of DVDs seized ______
Number of Flash devices seized ______
Number of other Items seized ______
Never take advice from the owner/user/suspect
Refer all questions to the investigator in charge
Never leave evidence unattended

Figure 2: Process Flow for Electronic Crime Scene

The process flow for seizing desktop computer hard disks is shown in Figure 3. The first question that arose in the development of this process flow was the handling of machines that are found running. Some literature support the removal of the power from the machine immediately [6] whilst other propagate some evidence collection first [2]. In this process flow an assisted shutdown is proposed. An assisted shutdown means that the normal operating system procedure is used to shutdown the machine gracefully, this can be done if a technically competent person is available to assist. In the absence of support the power plug is removed from the machine. It is argued that preserving the integrity of the potential evidence on the hard disk is much more important than any evidence that may be lost due to an immediate shutdown. It is further important to tie the suspect to the machine [11] and therefore an owner name and owner identity number is recorded.

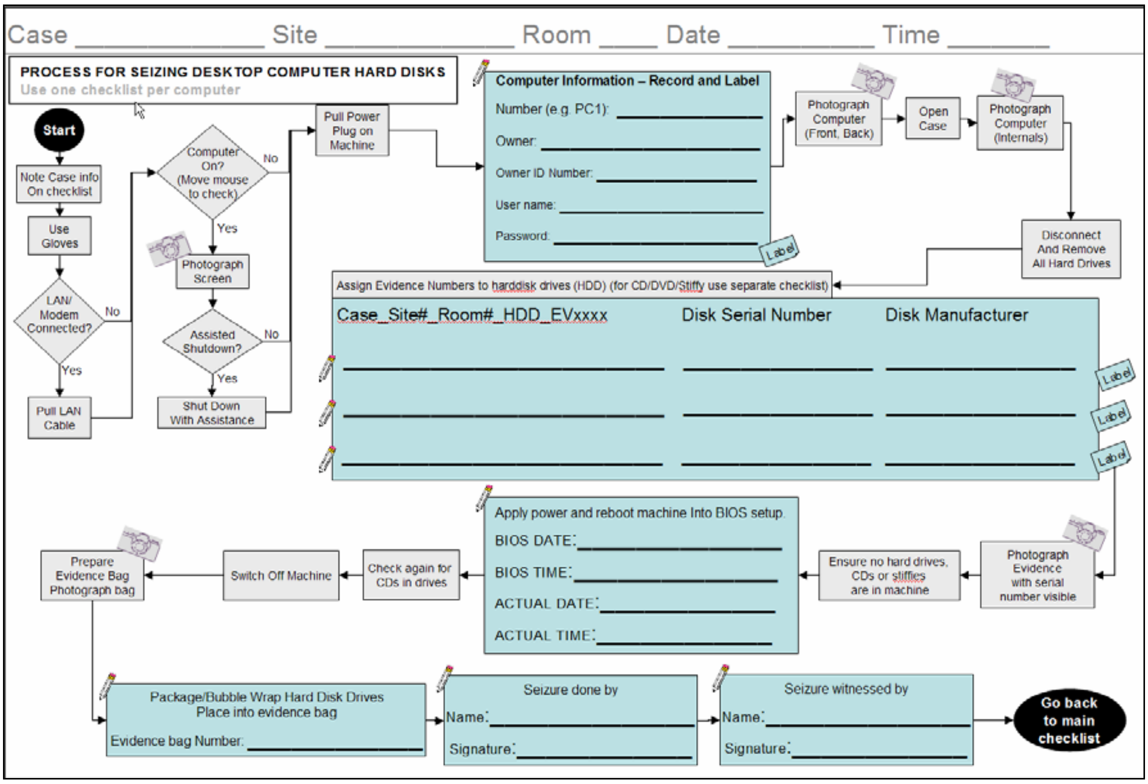

Case ______ Site ______ Room ____ Date ______ Time ______
PROCESS FOR SEIZING DESKTOP COMPUTER HARD DISKS
Use one checklist per computer
Start
Note Case info On checklist
Use Gloves
LAN/ Modem Connected?
No
Yes
Pull LAN Cable
Computer On? (Move mouse to check)
No
Yes
Photograph Screen
Assisted Shutdown?
No
Yes
Shut Down With Assistance
Pull Power Plug on Machine
Computer Information – Record and Label
Number (e.g. PC1):
Owner:
Owner ID Number:
User name:
Password:
Label
Photograph Computer (Front, Back)
Open Case
Photograph Computer (Internals)
Disconnect And Remove All Hard Drives
Assign Evidence Numbers to harddisk drives (HDD) (for CD/DVD/Stiffy use separate checklist)
Case_Site#_Room#_HDD_EVxxxx
Disk Serial Number
Disk Manufacturer
Label
Label
Label
Photograph Evidence with serial number visible
Ensure no hard drives, CDs or stiffies are in machine
Apply power and reboot machine Into BIOS setup.
BIOS DATE:
BIOS TIME:
ACTUAL DATE:
ACTUAL TIME:
Check again for CDs in drives
Switch Off Machine
Prepare Evidence Bag Photograph bag
Package/Bubble Wrap Hard Disk Drives Place into evidence bag
Evidence bag Number:
Seizure done by
Name:
Signature:
Seizure witnessed by
Name:
Signature:
Go back to main checklist

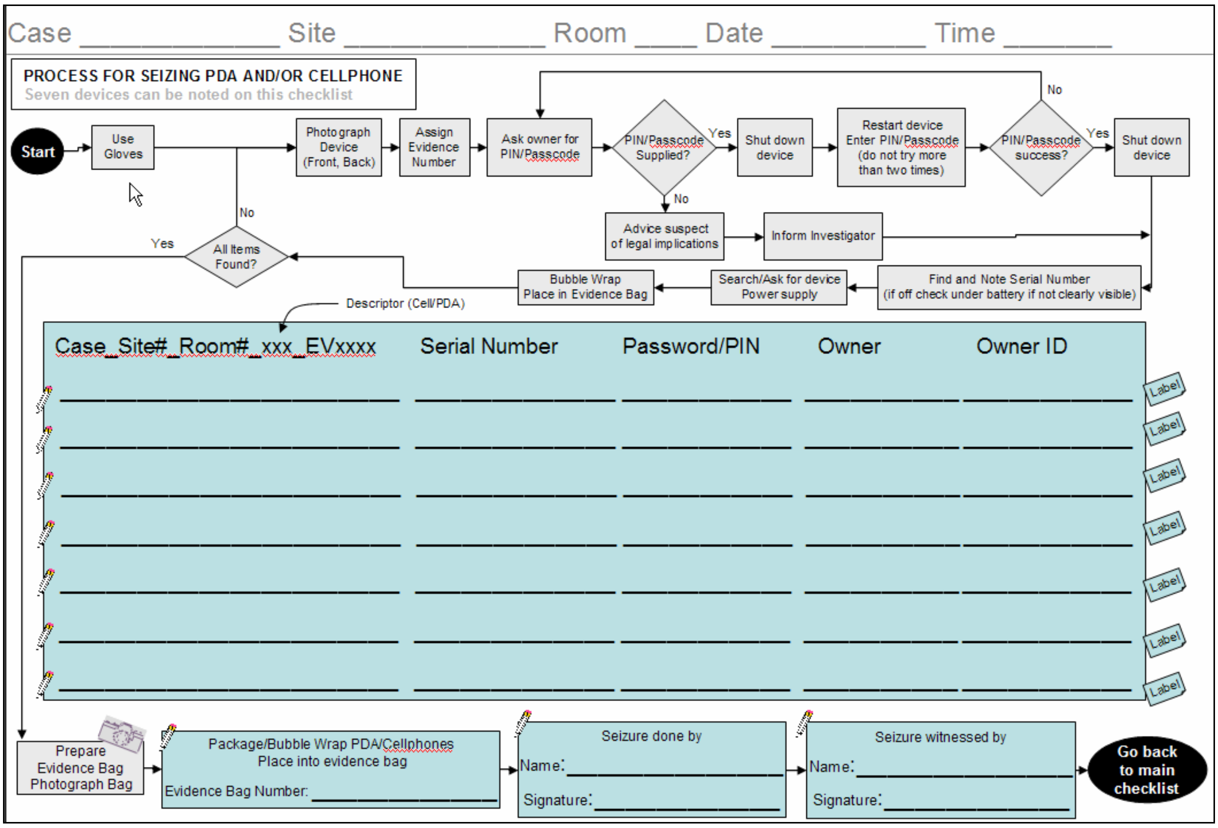
Figure 3: Process Flow for Seizing Desktop Computer Hard Disks

As mentioned earlier the front, back and inside of the computer is photographed. It is also important to note the machines BIOS date and time versus the actual date and time. This is necessary to link timestamp information found on files during analysis to the real time of the machine. In the process flow this is done after any devices (e.g. hard disks, stiffies, and CDs) are removed from the machine so as to ensure that potentially harmful programmes are not triggered on start up.

The general practice for which the process flows were developed only seize the hard disks from computers and not the total machine. This is proposed in order to minimise the transport and storage requirements. The hard disks can be analysed for evidence without the actual machine.

The process flow for seizing PDAs and/or Cell phones is shown in Figure 4. Cell phones and PDAs are grouped together due to their similar nature. For these devices it is important to obtain the necessary PIN or passcode as it is not possible, at least not without much effort and cost, to obtain evidence from these devices without it. If the owner of the device is uncooperative the investigator in charge of the scene must be notified. It will then be the decision of the investigator whether to take further action. It is important to note that the device is not shutdown if the PIN or passcode is not provided.

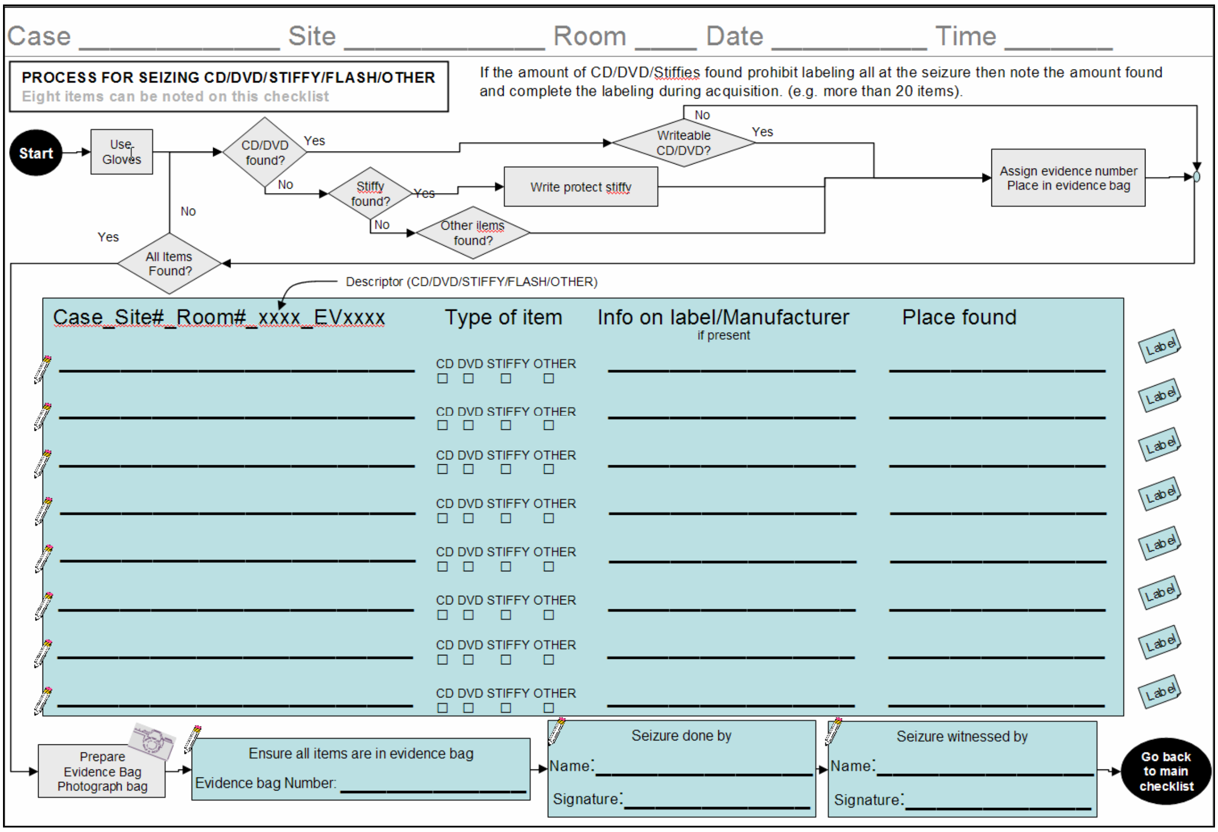
Cell phone and PDA devices typically require to be recharged within a relatively small space of time (e.g. a week or two). The power supply and connector configurations vary a lot between the different devices. In order to be able to recharge these devices for analysis the power supplies and/or chargers for these devices are also seized [6].



Case _____________ Site _____________ Room ____ Date __________ Time _______
PROCESS FOR SEIZING PDA AND/OR CELLPHONE
Seven devices can be noted on this checklist
Start
Use Gloves
Photograph Device (Front, Back)
Assign Evidence Number
Ask owner for PIN/Passcode
PIN/Passcode Supplied?
Yes
Shut down device
Restart device Enter PIN/Passcode (do not try more than two times)
PIN/Passcode success?
No
Yes
Shut down device
No
Advice suspect of legal implications
Inform Investigator
No
Yes
All Items Found?
Bubble Wrap Place in Evidence Bag
Search/Ask for device Power supply
Find and Note Serial Number (if off check under battery if not clearly visible)
Descriptor (Cell/PDA)
Case_Site#_Room#_xxx_EVxxxx
Serial Number
Password/PIN
Owner
Owner ID
Label
Label
Label
Label
Label
Label
Label
Prepare Evidence Bag Photograph Bag
Package/Bubble Wrap PDA/Cellphones Place into evidence bag
Evidence Bag Number: ____________
Seizure done by
Name: ____________
Signature: ____________
Seizure witnessed by
Name: ____________
Signature: ____________
Go back to main checklist

Figure 4: Process Flow for Seizing PDAs and Cell Phones

The process flow for seizing CD/DVD/STIFFY/FLASH/OTHER is shown in Figure 5. As most of these devices are non-volatile they are grouped together. It is possible that a large amount of these devices are found at the scene. Time may prohibit labelling all these at the scene. A note is placed on the process flow to indicate that such items can be seized together, placed into an evidence bag, and then later labelled as the acquisition takes place.



Case ____________ Site ____________ Room ____ Date __________ Time _______

PROCESS FOR SEIZING CD/DVD/STIFFY/FLASH/OTHER
Eight items can be noted on this checklist

If the amount of CD/DVD/Stiffies found prohibit labeling all at the seizure then note the amount found and complete the labeling during acquisition. (e.g. more than 20 items).

Case_Site#_Room#_xxxx_EVxxxx	Type of item	Info on label/Manufacturer if present	Place found
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________
______________________	CD □ DVD □ STIFFY □ OTHER □	________________	________________

Ensure all items are in evidence bag
Evidence bag Number: ____________

Seizure done by
Name: ____________
Signature: ____________

Seizure witnessed by
Name: ____________
Signature: ____________

Figure 5: Process Flow for Seizing CD/DVD/STIFFY/FLASH/OTHER

Some aspects suggested by other authors (e.g. BIOS passwords, network, encryption pass phrases [11], purpose of the system [6]) are not recorded on any of the process flows. There are two reasons for this. The first is that the A4 layout of the process flows does not provide sufficient space for all information to be recorded on the process flows. The second reason is that the amount of interaction between the

Cyber First Responder and any suspect must be minimised. This is to ensure that the suspect does not interfere with the process and potentially asks difficult questions that may undermine the confidence of the first responder which could lead to mistakes. Within the context of the process flow user environment the chief investigator is given the responsibility to interact in depth with any suspects.

V. Impact of the Process Flows

As mentioned earlier a Cyber Forensic First Responder course was developed. This course was presented to four groups of law enforcement personnel in South Africa. The courses were presented by the South African Council for Scientific and Industrial Research between February and April 2005. Each group consisted of 15 participants and the courses were presented by three lectures. The course combined theory and practice with the specific aim of developing a first responder that will have the skill and confidence to handle a cyber forensic search and seizure. Each participant was tested individually during a practical search and seizure and acquisition session. The results indicated if a participant passed, passed with supervision, or failed. The pass or pass with supervision rates for the four courses were 79%, 93%, 87%, and 80% respectively. It is difficult to compare these pass rates as the criteria for selecting participants was not exactly the same everywhere (some groups had more experience than other). Only in the last two training sessions were the process flows introduced.

The actual use of the process flows was lower than expected (53% in total with 60% of those who passed). Out of the pass rates it cannot conclusively be deduced that the process flows had a significant impact. The pass rates are however not the only measure of the success of the process flows. Other observations that were made over the four courses provide a better indication of the value of the process flows than the relation to passing. The first was a definite decrease in the seizure times. For the first course (although most of the participants had previous experience in cyber forensic seizures) most of the participants struggle to complete the seizure within the one hour time allocated. In the fourth course most of the participants could complete the seizure in less than one hour. The quickest seizure time dropped from 55 minutes in the first course to 40 minutes in the last course. The hypothesis formulated in section II was therefore confirmed.

In general participants who used the process flows were observed to: Complete the seizure in less time, make fewer mistakes, were more relaxed, and were more confident.

In the course feedback sessions participants were asked if the process flows was useful and if they preferred it vs. checklists. In all cases the participants preferred the process flows and indicated that they would use it in operational activities.

VI. Conclusion

In this paper the authors indicated the requirement for cyber forensics training and the lack of skilled resources with a technical background on information technology was highlighted. It was further indicated that process and information support is available but not in a format suitable for use by individuals who are not formally trained in ICT. The definition and use of process flows during cyber forensic search and seizures was introduced and the benefits of the process flows were illustrated.

The hypothesis that the process flows would speed up the search and seizure process was tested and confirmed. The use of the process flows increased the confidence of the first responders and decreased seizure times.

Some enhancements can still be made to the process flows, an example being a means to indicate a photo number, or other reference, on the process flows. Adding an acquisition process flow will also be beneficial. An acquisition process flow's structure will depend on the actual hardware and software being used. Some environments would want to customise the existing process flows. A process flow detailing the actions to follow if the acquisition is to take place on site may also be needed. This work has indicated certain important aspects of the process flows that should be taken into account when developing, customizing, or evaluating process flows. The first set of process flows is generic in the sense that it does not rely on the use of any specific hardware or software, future process flows may not be so generic. The basic structure of the process flows indicated in Figure 1 support the future development of new process flows whilst keeping to a format that First Responders can easily recognise and understand.

Although the use of mobile computers for record purposes during seizures is not currently common practice, at least not in the South African context, this could change in future. The process flows can ideally be implemented in software for use on a mobile computer. This will enable even better management of the seizure process through the prompting of specific actions. Such a tool can support the collection of more information for which the hard copy based process flows can not make provision for. The information capture can also automatically be fed into a case management tool. This will not only improve efficiency but decrease the possibility of mistakes.

In general it can be concluded that the process flows is beneficial to first responders performing cyber forensic search and seizures.

VII. References

[1] Beebe, N.L., Clark, J.G., *A Hierarchical, objectives-based framework for the digital investigation process,* Digital Investigation, Elsevier, 2005.

[2] Brezinky, D., et al, *RFC 3227 – Guidelines for Evidence Collection and Archiving*, The Internet Society, 2002.

[3] Institute for Security Technology Studies at Dartmouth College, *Law Enforcement Tools and Techniques for Investigating Cyber attacks: A National Needs Assessment,* June 2002.

[4] NHTCU, *Hi-Tech Crime: The Impact on UK Business 2005,* NHCTU, 2005.

[5] Rogers, M. K., *The future of computer forensics: a needs analysis survey,* Computers and Security, Volume 23, Issue 1, Elsevier, February 2004.

[6] US Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders,* July 2001.

[7] Vacca, J.R., *Computer Forensics – Computer Crime Scene Investigation,* ISBN 1-58450-018-2, Charles River Media, 2002.

[8] Wolfe, H. B., *Forensics evidence testimony – some thoughts*, Computers and Security Vol. 22, No. 7, Elsevier, 2003.

[9] Wolfe, H. B., *Setting up and electronic evidence forensics laboratory,* Computers & Security Vol. 22 NO. 8, Elsevier, 2003.

[10] Wolfe, H.B., *Computer Forensics,* Computers & Security, Elsevier, 2003.

[11] Wolfe, H.B., *The circumstances of Seizure,* Computers & Security, Elsevier, 2003.