Chapter 26

PROCESS FLOW DIAGRAMS FOR TRAINING AND OPERATIONS

Jacobus Venter

Abstract This paper focuses on the use of process flow diagrams for training first responders who execute search and seizure warrants at electronic crime scenes. A generic process flow framework is presented, and the design goals and layout characteristics of process flow diagrams are discussed. An evaluation of the process flow diagrams used in training courses indicates that they are beneficial to first responders performing searches and seizures, and they speed up investigations, including those conducted by experienced personnel.

Keywords: Process flow diagrams, first responders, search and seizure

1. Introduction

The rapid development and use of information and communications technology have influenced everyday life, mostly in a positive manner. However, the technology is also being exploited for criminal purposes. Computer-related crime is very significant—according to a recent study, the monetary impact of high tech crime in the United Kingdom in 2004 exceeded £2 billion [4]. This situation has resulted in an increased demand for personnel with digital forensics expertise in law enforcement and other government agencies.

Responding to the need for trained personnel, the South African Government instituted several digital forensics training programs. However, the task is complicated by the lack of personnel with adequate expertise or formal training in information and communications technology. This is true internationally: in the United States, for example, only a small number of investigative units have computer scientists or other technically trained individuals on staff [3]. Therefore, it is often the case that

existing personnel, even those without advanced technical skills, must be trained in digital forensics prior to working in the field.

This paper focuses on training first responders who are responsible for collecting items that may contain electronic evidence. In the South African context, first responders are specially-trained investigators or inspectors who normally act on search and seizure warrants. Before undergoing training, most of these individuals have limited understanding about electronic crime scenes and little expertise in computers and electronic devices. Therefore, it is important to develop effective training regimens for individuals with limited background and technical skills.

Electronic crime scene handling procedures are generally presented in the form of descriptions or lists (see, e.g., [2, 6, 7]). Much of the literature provides general principles, but first responders need detailed guidance. In many cases, when detailed steps are provided, they presume expertise in information and communications technology. For example, one of the steps in RFC 3227 [2] is: "For each system, obtain the relevant order of volatility." This assumes that first responders know the volatilities of systems and can prioritize them.

In our experience, this was definitely not the case for most trainees from law enforcement agencies. Some of the trainees, for example, spent inordinate amounts of time seizing CDs and then rushed through the process of seizing hard disks, which are much more important. The well-known U.S. Department of Justice guide for first responders [6] provides detailed, sequenced information, but the information is spread over several pages. We observed that first responders often did not refer to this information during seizure. Also, because the information was spread over several pages, they used some of it in the wrong context.

This paper discusses a process flow strategy, which we created to address deficiencies inherent in first responder training programs and to support operations. First, we developed a model of the tasks that had to be performed by first responders. This model was articulated in terms of process flow diagrams, which were subsequently tested in training courses offered to first responders with limited expertise in information and communications technology.

2. Motivation

Building the skills of digital forensics professionals requires ongoing attention. A 2001-02 national needs assessment on law enforcement tools and technologies conducted by the Institute for Security Technology Studies at Dartmouth College [3] noted that training programs that fit law enforcement needs were a specific requirement. This view was

reinforced in a 2004 study by Rogers and Seigfried [5], which indicated that education/training and certification were major needs. The same viewpoint was also expressed by a special investigation unit in the South African law enforcement community.

First responders need to understand the basic actions to be taken upon encountering an electronic crime scene. Several manuals have been developed to train and assist first responders. A good example is the U.S. Department of Justice guide for first responders [6], which provides excellent information on handling electronic crime scenes. However, the guide is not very useful to first responders with limited expertise in information and communications technology.

We have developed process flow diagrams to address this problem. The process flow diagrams provide structured paths of actions for first responders to follow and to check off as they are taken. Process flow diagrams also speed up investigations, including those conducted by experienced personnel.

Beebe and Clark [1] argue that digital investigation frameworks should not use a checklist approach—each situation is likely to be unique and different steps may have to be taken in each situation. Since process flow diagrams are checklist-oriented, they are subject to critique. We argue, however, that the target audience for the process flows requires a more rigorous approach that will deal adequately with most situations. This view is supported by RFC 3227 [2], which suggests that the number of decisions made during the collection process must be minimized. Additional support comes from Wolfe [9], who emphasizes that following a process decreases the probability of making errors and facilitates good documentation. Individuals without sufficient technical qualifications and experience should not deviate from the prescribed steps because they may not be able to explain the implications in courtroom testimony. We also argue that a process flow diagram adds sequence to actions in a manner that is easier to understand than a detailed list. On the other hand, we believe the objectives-based approach of Beebe and Clark [1] is well suited to complex situations and advanced phases of the forensic process. Indeed, we use process flow diagrams for situations that do not involve complex configurations or environments.

3. Design Goals and Layout Characteristics

This section discusses the design goals and layout characteristics for process flows. The actual process flow diagrams created for first responders are presented in the next section.

The first design goal was ease of use by individuals with limited expertise in information and communications technology. Digital forensics is a highly technical field, but many first responders do not have adequate knowledge and skills. Consequently, the focus was to develop process flow diagrams that would enable non-technical individuals to perform adequately in the majority of cases.

The second design goal was to create process flow diagrams applicable to the most likely cases. Developing process flows to deal with the variety of equipment, installations and configurations found at crime scenes is not be feasible. Therefore, the diagrams were built around common equipment and frequently occurring scenarios. The scenarios used to create the process flows were based on more than 50 cases.

The third design goal was to ensure that the process flow diagrams, at the very least, would not interfere with expert testimony, and, if possible, strengthen the testimony. Therefore, the design of the diagrams had to take into account potential evidentiary challenges arising from the actions of first responders. It is in this context that the checklist nature of the process flow diagrams could be problematic, especially if a checklist is not followed exactly and the first responder cannot explain why the deviation occurred. We argue that, given the target users of the process flow diagrams, it is more important to ensure that a first responder can testify confidently about the process than his ability to handle exceptions. Wolfe [10] notes that a good attorney can rattle or confuse any witness, reducing the value of the testimony or negating it altogether. He also emphasizes that close attention must be paid to following and documenting the forensic methodology [11]. Process flow diagrams support this by providing well documented methodologies for searches and seizures, and they assist first responders in reporting on their actions with confidence.

The final design goal was to create process flow diagrams that could be used during operations as well as training. Indeed, in our training sessions, many participants mentioned that they intended to use the process flows in operations.

In addition to the design goals, certain layout characteristics of the process flow diagrams are worth mentioning. The first characteristic is that each process flow must be reproducible in black and white, and should fit on a single A4 page. This layout facilitates duplication, and allows the process flow diagrams to be compiled in a normal A4 record book.

Recording information is vital throughout the forensic process, including during the evidence collection phase [2]. The process flows support this aspect by ensuring that important information is captured when

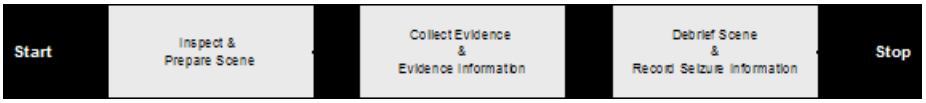

Figure 1. Generic framework elements.

following the steps in a process flow diagram. All information recorded is clearly associated with a specific case, site and room, because these are all recorded in the process flows.

Certain naming conventions are indicated in the process flow diagrams. These remind first responders about the correct naming conventions for specific pieces of evidence. For example, the process flow diagram for seizing storage media (Figure 5) employs the naming convention Case_Site#_Room#_xxxx_EVxxx. The descriptor used for the first xxxx part is "CD/DVD/STIFFY/FLASH/OTHER." This naming convention, which is used throughout the South African system, clearly identifies the origin of evidentiary material.

4. Process Flow Diagrams

This section describes the four process flow diagrams that were developed for first responders. One process flow deals with general behavior at electronic crime scenes; the remaining three cover specific types of devices.

Figure 1 presents the generic framework elements in each of the process flows. The three elements are: "Inspect & Prepare Scene," "Collect Evidence & Evidence Information," and "Debrief Scene & Record Seizure Information."

The "Inspect & Prepare Scene" element contains actions to prepare first responders for the tasks to follow (e.g., "Use Gloves" in Figures 3, 4 and 5), actions to survey the scene (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 evidence (e.g., "Write Protect Stiffy" in Figure 5). Note that in South Africa, 3.5-inch floppy disks are known as "stiffies" because they are stiffer than the older 5.25-inch floppies.

The actions in the "Collect Evidence & Evidence Information" element revolve around recording information related to specific evidentiary aspects (e.g., "Computer Information – Record and Label" in Figure 3), assigning unique identifiers to evidentiary items (e.g., "Assign evidence number, place in evidence bag" in Figure 5), and noting special infor-

mation (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 evidentiary items (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 individuals 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 for first responders because the same basic steps are followed for all categories of evidence.

The first general aspect is recording information in process flow diagrams. RFC 3227 [2] indicates that where and when the evidence was discovered and collected, and who discovered and collected the evidence must be noted. These are addressed in two ways. First, at the top of all the process flow diagrams, the CASE, SITE, ROOM, DATE and TIME details are captured. Second, information is captured within the process flows themselves. See, e.g., the space for noting the details of the individuals who performed the seizure and witnessed the seizure in Figures 2, 3 and 4.

The second general aspect is using cameras. Photographs are useful and important [6–8]. In all the process flow diagrams, photo points are shown with a  icon. Photographs assist in documenting the exact setup of the equipment, screenshot, cabling, peripheral devices, etc. They also help solve disputes that might occur later. For example, the owner of a seized computer might contend that the one presented as evidence is not the one that was actually seized. Detailed photographs taken at the crime scene would quickly resolve the issue.

Figure 2 shows the process flow diagram for responding to an electronic crime scene. This process flow begins by verifying the search warrant: it is necessary to verify that the warrant covers the applicable electronic devices searched for and seized by the first responder. The next step in the process flow is to separate all persons from computer equipment as soon as possible [9]. The rest of the process flow focuses on identifying and recording the evidence, and directs first responders to the appropriate detailed process flow diagram. The sequence, PC then PDA or cell phone, then CD/DVD, stiffy/flash, other, is a form of prioritization. Computer hard disks hold the most data and are the most likely source of evidence. Next are PDAs and cell phones that may contain valuable contact information. The last is other storage devices. Special reminders, e.g., "Never leave evidence unattended," are also indicated in the process flow diagram.

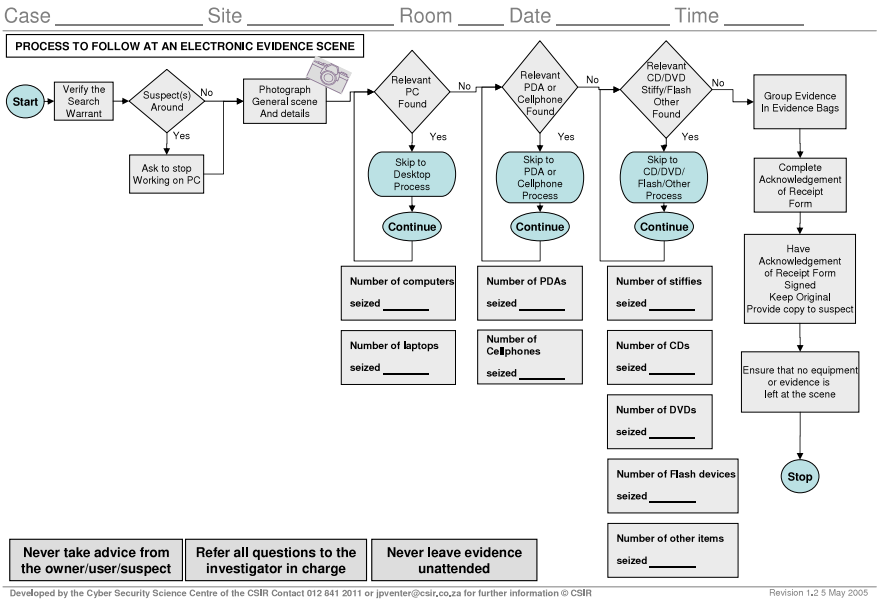

Figure 2. Process flow diagram for an electronic crime scene.

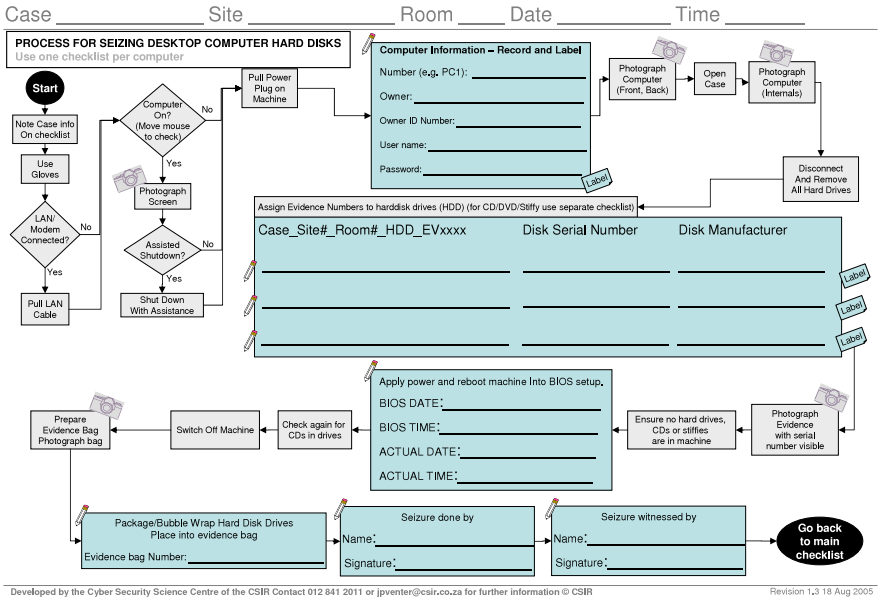

Figure 3. Process flow diagram for seizing desktop computer hard disks.

The process flow diagram for seizing desktop computer hard disks is shown in Figure 3. The first question that arose during its development was how to handle machines that are found to be running. Some experts recommend the immediate removal of the power cord from the machine [6], while others stress that evidence must be collected first [2]. The process flow in Figure 3 proposes an assisted shutdown: the normal operating system procedure is used to shut down the machine gracefully only if a technically competent person is available to assist. In the absence of technical support, the power cord should be removed from the machine. The rationale is that preserving the integrity of potential evidence on the hard disk is much more important than any volatile evidence that may be lost due to an immediate shutdown. Since it is important to tie the suspect to the machine [9], the owner's name and identifying number must be recorded.

Other tasks to be performed are photographing the front, back and insides of the computer, and noting the machine's BIOS date and time versus the actual date and time. This is necessary to connect file timestamps to the actual time of file access during the forensic analysis phase. The process flow diagram requires these tasks to be performed after all devices (e.g., hard disks, stiffies and CDs) are removed from the machine to ensure that potentially harmful programs are not triggered upon start up.

Figure 4 presents the process flow diagram for seizing PDAs and cell phones. These devices are grouped together due to their similar nature. It is important to obtain the PINs or passcodes of the devices as it is not possible—without much effort and cost—to obtain evidence without them. If the owner of a device is uncooperative, the investigator in charge of the scene must be notified. It is then up to the investigator to take further action. Note that the device must not be shut down if the PIN or passcode is not available.

PDAs and cell phones typically have to be recharged relatively soon (e.g., a week or two). Since the power supply and connector configurations are often unique to the devices, they must also be seized so that the devices can be recharged (if necessary) during the analysis phase [6].

The process flow diagram for seizing other non-volatile storage media is shown in Figure 5. Since a large number of these devices are often found at a crime sceme, it may not be possible to label all of them at the scene. Therefore, the process flow diagram indicates that these items may be seized together, placed in an evidence bag, and labeled later.

Certain items suggested by other authors, e.g., BIOS passwords, encryption pass phrases [9], and the purpose of the system [6], are not recorded on any of the process flow diagrams. There are two reasons for

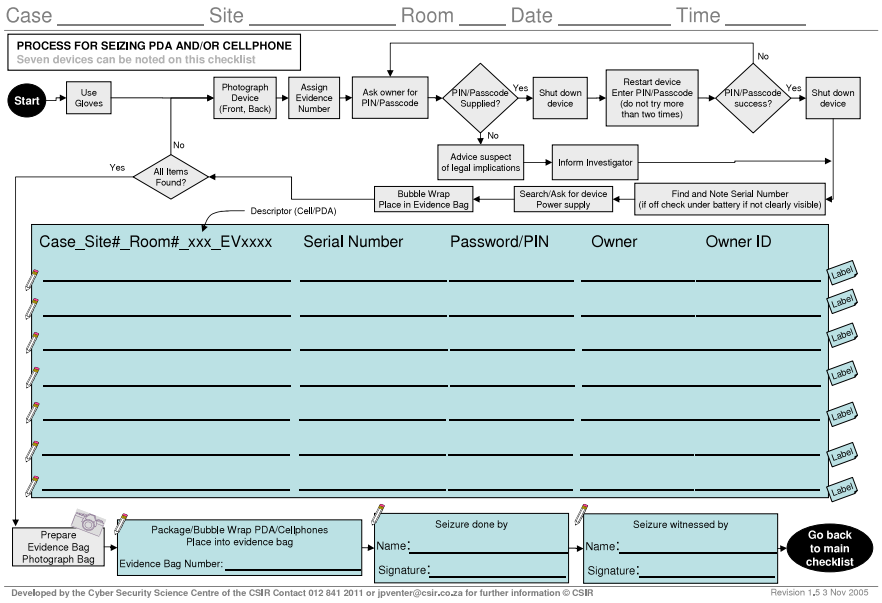

Figure 4. Process flow diagram for seizing PDAs and cell phones.

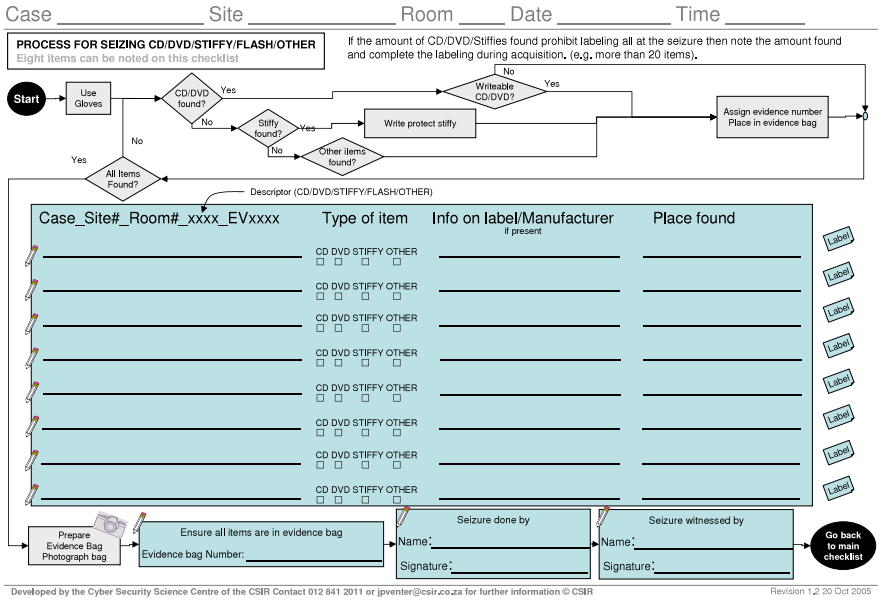

Figure 5. Process flow diagram for seizing non-volatile storage media.

this. The first is that the A4 layout does not provide enough space for all information to be recorded on the process flows. The second reason is that interactions between a first responder and a suspect should be minimized; this is to ensure that the suspect does not interfere with the process and possibly undermine the confidence of the first responder, which could lead to mistakes. We assume that the chief investigator—not the first responder—is responsible for interacting at length with suspects.

5. Impact of Process Flow Diagrams

A digital forensics course for first responders was developed and taught to four groups of law enforcement personnel in South Africa. The courses were presented by the South African Council for Scientific and Industrial Research from February through April 2005. Each group consisted of 15 participants and the courses were presented by three lecturers. The courses combined theory and practice with the specific aim of developing first responders who would have the skills and confidence to conduct searches and seizures involving digital evidence. Each participant was tested individually during a practical search and seizure session.

The process flow diagrams were developed during the first two training courses, and were tested on trainees during the third and fourth courses. The use of the process flow diagrams during the practical tests was lower than expected (53% total; 60% of those who passed). Based on the pass rates, it cannot be concluded that the process flows had a significant impact.

However, other observations made during the training courses provide better indicators of the impact of process flow diagrams. The first was a noticeable decrease in seizure times. In the first course, where process flows were not used, although most of the participants had previous experience, many still struggled to complete the seizure test within the one hour allocated to them. In the fourth course, where the process flow diagrams were used, most of the participants completed the seizure test in less than one hour. The quickest seizure time dropped from 55 minutes in the first course to 40 minutes in the fourth course.

In general, participants who used the process flow diagrams completed the seizures in less time, made fewer mistakes, and were more relaxed and confident. During the course feedback sessions, participants indicated that they preferred the process flow diagrams over traditional checklists, and mentioned they would use them in their operational activities.

6. Conclusions

Process flow diagrams are a powerful means for detailing the actions that first responders must perform when executing search and seizure warrants at electronic crime scenes. The evaluation of process flows indicates that are useful for training individuals with limited expertise in information and communications technology. Using process flow diagrams also contributed to increased confidence on the part of first responders and faster seizure times. Moreover, process flows have significant operational value, and often speed up investigations by experienced law enforcement personnel.

Several enhancements are possible. These range from incorporating a means to indicate photo numbers and other references in process flows to creating an acquisition process flow diagram, which details the actions to be performed during an on-site acquisition of evidence. Our basic process flow structure supports the development of new process flow diagrams while preserving the simplicity desired by first responders. Other enhancements include customizing process flow diagrams, and using them in conjunction with a computerized case management system. This would improve the quality and efficiency of searches and seizures, as well as every phase of the digital forensic process—from evidence acquisition and examination to analysis and courtroom presentation.

References

[1] N. Beebe and J. Clark, A hierarchical, objectives-based framework for the digital investigation process, *Digital Investigation*, vol. 2(2), pp. 147-167, 2005.

[2] D. Brezinky and T. Killalea, Guidelines for evidence collection and archiving, RFC 3227, The Internet Society, 2002.

[3] Institute for Security Technology Studies, Law Enforcement Tools and Techniques for Investigating Cyber Attacks: A National Needs Assessment, Technical Report, Dartmouth College, Hanover, New Hampshire, 2002.

[4] National Hi-Tech Crime Unit, High-tech crime: The impact on UK business—2005, London, United Kingdom, 2005.

[5] M. Rogers and K. Seigfried, The future of computer forensics: A needs analysis survey, *Computers & Security*, vol. 23(1), pp. 12-16, 2004.

[6] U.S. Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, Washington, DC, 2001.

[7] J. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, Charles River Media, Hingham, Massachusetts, 2002.

[8] H. Wolfe, Computer forensics, *Computers & Security*, vol. 22(1), pp. 26-28, 2003.

[9] H. Wolfe, The circumstances of seizure, *Computers & Security,*, vol. 22(2), pp. 96-98, 2003.

[10] H. Wolfe, Forensics evidence testimony—Some thoughts, *Computers & Security*, vol. 22(7), pp. 577-579, 2003.

[11] H. Wolfe, Setting up an electronic evidence forensics laboratory, *Computers & Security*, vol. 22(8), pp. 670-672, 2003.