

Field Guide Part Four

Timothy Wright 2000-09-01

Last time...

In our last article, [Search and Seizure Basics](#), we discussed six fundamental rules that an investigator should always have in mind when performing a search and seizure. Primarily, these rules are to help establish and safeguard the chain of custody for computer crime scene evidence. At this juncture, we're ready to look at the first stage of the search and seizure process: planning.

Planning and the Computer Search (Warrant) Team

Here, two critical issues must be brought to light: first, there is a measure of planning that should take place before any investigator steps foot in a computer crime scene, and second, the roles and responsibilities of the investigators who interact with the crime scene must be outlined. It is essential to understand that "forensic science begins at the crime scene" [1, pg. 37]. The endeavor of securing and collecting evidence plays a major role in the overall investigative process. Hence, any forethought and strategy preceding this activity will serve to bolster further forensic work.

Planning

(A)	(B)	(C)	(D)	(E)	(F)
Formulate plan	Approach and Secure Crime Scene	Document Crime Scene Layout	Search for Evidence	Retrieve Evidence	Process Evidence

Figure 1: Planning - Stage A of a Search and Seizure

Prior to any team of investigators arriving at the crime scene, a plan of action should be thoroughly considered. In particular, the FBI lists the following suggestions in reference to crime scenes in general [2, pg. 15]:

1. Accumulate the packaging and materials necessary for typical search circumstances
2. Prepare the preliminary format for the paperwork needed to document the search
3. Ensure that all specialists are aware of the overall forms of evidence usually encountered as well as the proper handling of these materials
4. Evaluate the current legal ramifications of crime scene searches
5. Discuss the search with involved personnel before arrival at the scene, if possible
6. Identify, when feasible, a person-in-charge prior to arrival at the scene
7. Make preliminary personnel assignments before arrival at scene, if practicable
8. Consider the safety and comfort of search personnel. When encountering a potentially dangerous scene or inclement weather, be prepared...
9. Assess the personnel assignments normally required to process a crime scene successfully

Each of these suggestions has implications which can make or break an investigation. However, regarding computer crime, the first four warrant a closer look.

Planning Suggestion 1: Accumulate the Packaging Materials

Where computer hardware and software are concerned, appropriate packaging materials are crucial. In particular, anti-static, plastic covers; packing foam; and sturdy cardboard boxes will go a long way to ensure safe transport of evidence from the field to the lab. Additionally, appropriate containers for diskettes, CDs, tapes and other storage devices are essential to protect these media from physical damage and provide organization. Other materials necessary for interacting with a computer crime scene can include: a camera (e.g., instant-development, 35-mm, video), investigation computers (e.g., notebooks, sub-notebooks), networking cables and hardware, and investigation software (e.g., boot diskettes, boot CDs).

Planning Suggestion 2: Prepare the Preliminary Format for the Paperwork Needed to Document the Search

Perhaps a better idea than utilizing paper to document a crime scene is to use some form of electronic documentation. Either way, having the necessary means for documentation ready to go will save time and confusion at the crime scene. For a search and seizure there are two logs (electronic or paper) which are needed initially: the **search and seizure evidence log**, and the **shipping manifest**. The former is used at the crime scene to track information about computer evidence, while the latter is used to account for evidence that is shipped from the crime scene to the evidence preservation lab. Ultimately, after evidence is brought back to the

lab, a third log file, the lab evidence log, is created. Similar to the search and seizure evidence log, the lab evidence log tracks data about computer evidence as the evidence is examined. We'll look more closely at each log later on. Note that good case management software can provide the investigator with access to all necessary log files under one convenient, graphical interface. As mentioned earlier, such software is a far better choice than using spreadsheets or paper!

Planning Suggestion 3: Ensure that All Specialists Are Aware of the Overall Forms of Evidence

If investigators do not understand what they will be dealing with at the crime scene, there is a good chance that evidence will be mishandled, and the chain of custody will be disturbed. Similarly, if the investigators are inadequately equipped to collect and manage evidence at the crime scene, both the evidence and the chain of custody can again be damaged. To ensure the integrity of their forensics work, investigators should be properly educated about a given crime scene, in advance of their arrival. Along these lines, Richard Saferstein notes that, "the competence of a laboratory staff and the sophistication of its analytical equipment have little or no value if relevant evidence cannot be properly recognized, collected, and preserved at the site of a crime" [1, pg. 22].

Planning Suggestion 4: Evaluate the Current Legal Ramifications of Crime Scene Searches

Be cognizant of the privacy rights of suspects! Except in some circumstances, law enforcement officials should have a court approved search warrant. In theory, corporate investigators should not have any legal difficulty collecting evidence that is owned by their corporation. Yet, they should always consult their corporation's legal department to understand the limits of their investigation. In particular, investigators should be cautious of the legal ramifications of accessing stored electronic communications on a server. This situation is covered by the Electronic Communications and Privacy Act (U.S. Criminal Code and Rules, Title 18, Sections 2701 - 2711) [3]. In their book, *Investigating Computer Crime*, Clark and Diliberto note the following example [4, pg. 35]:

...a bulletin board provides confidential e-mail exchanges between members. Evidence shows that information which constitutes a crime is being sent between several members but no information exists showing that the system operator is involved in criminal activity. The search warrant would have to be limited by the facts and to mail between the parties involved in criminal activity. Taking and/or searching the entire computer including the e-mail of parties

not involved in crimes is a violation of the Electronic Communications Privacy Act.

In addition to the FBI's nine suggestions for planning, it may also be useful to evaluate the computer crime scene prior to any investigators showing up there. For example, by knowing ahead of time the locations and quantities of various computers and peripherals, the activities at a computer crime scene will be more streamlined and evidence less susceptible to contamination. Clark and Diliberto suggest obtaining or creating a map of the crime scene to assist with this evaluation [4, pg. 51]. In particular having this information will provide insight into the packaging materials needed, the forms of evidence that might be encountered, and the kind of search that will need to be performed.

The Computer Search (Warrant) Team

Having looked at options and suggestions for planning a search and seizure, we now turn our attention to delegating responsibilities within the search and seizure team. There are two team models explored in detail below: that proposed by Clark and Diliberto, and a more streamlined model proposed by the FBI.

The Clark and Diliberto Search Team Clark and Diliberto refer to the investigators dispatched to the computer crime scene as the "Computer Search Warrant Team [4, pg. 9]" (although, in a corporate setting, a warrant may not be required). The preferred makeup of such a team is described in Table 1.

Table 1: Clark and Diliberto's Computer Search Warrant Team

Role	Duties
Case Supervisor	<ul style="list-style-type: none"> • Handle media relations • Manage and schedule manpower and equipment needs • Oversee case
Interview Team	<ul style="list-style-type: none"> • Interview witnesses and suspects

Sketch and Photo Team	<ul style="list-style-type: none"> • Sketch the search scene • Assign room letters • Photograph entire scene inside and out • Photograph all evidence
Physical Search Team	<ul style="list-style-type: none"> • Search all rooms • Mark all evidence with colored stick-on dots for easy location by Seizure Team
Security and Arrest Team	<ul style="list-style-type: none"> • Provide physical security of crime scene entrances, and evidence
Technical Evidence Seizure and Logging Team	<ul style="list-style-type: none"> • Seize evidence • Log evidence data • Label and place evidence in bags or boxes (after evidence is photographed) • Take down computer systems after area is secure and computer has been photographed

On the Computer Search Warrant Team, the Case Supervisor bears overall responsibility for team activities, although he or she "may not have to stay at the scene beyond the initial entry and securing of the scene" [4, pg. 9]. As the Interview, Sketch and Photo, and Security and Arrest teams execute their functions, the Technical Evidence Seizure and Logging Team should assess the dispositions of all crime scene computers. This information should be documented, RAM drives should be identified, and then the process of shutting down these computers should begin. Upon tagging and labeling all computer components (and allowing this evidence to be photographed), the Technical Evidence Seizure and Logging Team should proceed to pack carefully the evidence for transport. Clark and Diliberto suggest that when the Physical Search Team marks evidence, a different color sticker bearing team member initials should be used for each room to further establish the chain of custody [4, pg. 48]. Along these same lines, Saferstein points out the following [1, pg. 48]:

If at all possible, the evidence itself should be marked for identification. Normally, the collector's initials and the date of collection are inscribed directly on the article. However if the

evidence collector is unsure of the necessity of marking the item itself, or has doubts as to where to mark it, it is best to omit this step.

The FBI Search Team

The Computer Search Warrant Team proposed by Clark and Diliberto, although thorough, is somewhat cumbersome. The FBI proposes a more streamlined crime scene team with the roles and responsibilities outlined in Table 2 [2, pg 15].

Table 2: FBI's Computer Search Team

Role	Duties
Person-In-Charge	<ul style="list-style-type: none"> • Administrative log • Narrative description • Preliminary Survey • Scene security • Final Decision making
Photographer	<ul style="list-style-type: none"> • Photographs • Photographic log
Sketch Preparer	<ul style="list-style-type: none"> • Sketch • Documentation of items on sketch
Evidence Recorder	<ul style="list-style-type: none"> • Evidence log • Evidence custodian

As with the Case Supervisor on the Clark and Diliberto search team, the Person-In-Charge on the FBI's computer search team should manage the crime scene and the activities taking place there. Additionally, this role is tasked with creating a narrative description of the crime scene, conducting the preliminary crime scene survey, and managing security. The narrative description is, "a running, written description of the condition of the crime scene in general terms" [2, pg. 17]. The preliminary survey is primarily an organizational measure to plan for a more comprehensive search. In essence, this includes a cautious walk through the crime scene, preliminary photographs, a determination of how the comprehensive search should be carried

out, and, of course, "extensive notes" [2, pg. 16]. As with Clark and Diliberto's search team, the Photographer and Sketch Preparer can perform their functions simultaneously with the rest of the search team's duties with two exceptions: first, photographs of computer evidence must be taken before that evidence is packaged for transport, and second, as it is located the Sketch Preparer should place evidence into the crime scene sketch. Finally, the Evidence Recorder is analogous to the Technical Evidence Seizure and Logging Team in the Clark and Diliberto team architecture. It is up to the Evidence Recorder to carefully document all collected electronic evidence, and prepare this evidence for transport to an evidence preservation lab.

Next Time...

In this installment of The Field Guide for Investigating Computer Crime, we've made the transition from overview and background information, to a discussion of the first stage of the search and seizure process: Planning. We found that at this juncture the preparation and team structuring activities that take place, help to ensure a successful investigation. Without these activities, the chain of custody is put at great risk.

In our next few articles, we'll continue on with the stages for a search and seizure. Along the way, we'll discuss the three log files that were introduced above for documenting a search and seizure, and we'll give some consideration to the threat that viruses pose to forensics work. Finally, the steps for processing computer crime scene evidence will be presented.

To read **The Field Guide for Investigating Computer Crime: Search and Seizure Approach, Documentation, and Location (Part 5)**, click [here](#).

References

- (1) Saferstein, Richard. "Criminalistics: An Introduction to Forensic Science, Sixth Edition," Prentice Hall, Upper Saddle River, New Jersey, 1998.
- (2) Federal Bureau of Investigation, U.S. Department of Justice. "Handbook of Forensic Science," U.S. Government Printing Office, Washington D.C., 1994.
- (3) "1998 Edition Federal Criminal Code and Rules," West Group, St. Paul, 1998
- (4) Clark, Franklin and Diliberto, Ken. "Investigating Computer Crime," CRC Press, New York, 1996.

For the past several years, [Timothy Wright](#) has been investigating computer fraud and abuse as a Senior Technology Investigator at one of the country's largest financial corporations. Before then, he worked as a lead developer within the financial industry, designing and building web-based home banking software. He holds an M.S. in Computer Science, and a B.A. in Philosophy.

Relevant Links

[An Introduction to the Field Guide for Investigating Computer Crime \(Part 1\)](#)

Timothy Wright

[The Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics \(Part 2\)](#)

Timothy Wright

[The Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics \(Part 3\)](#)

Timothy Wright

[Privacy Statement](#)

Copyright 2006, SecurityFocus