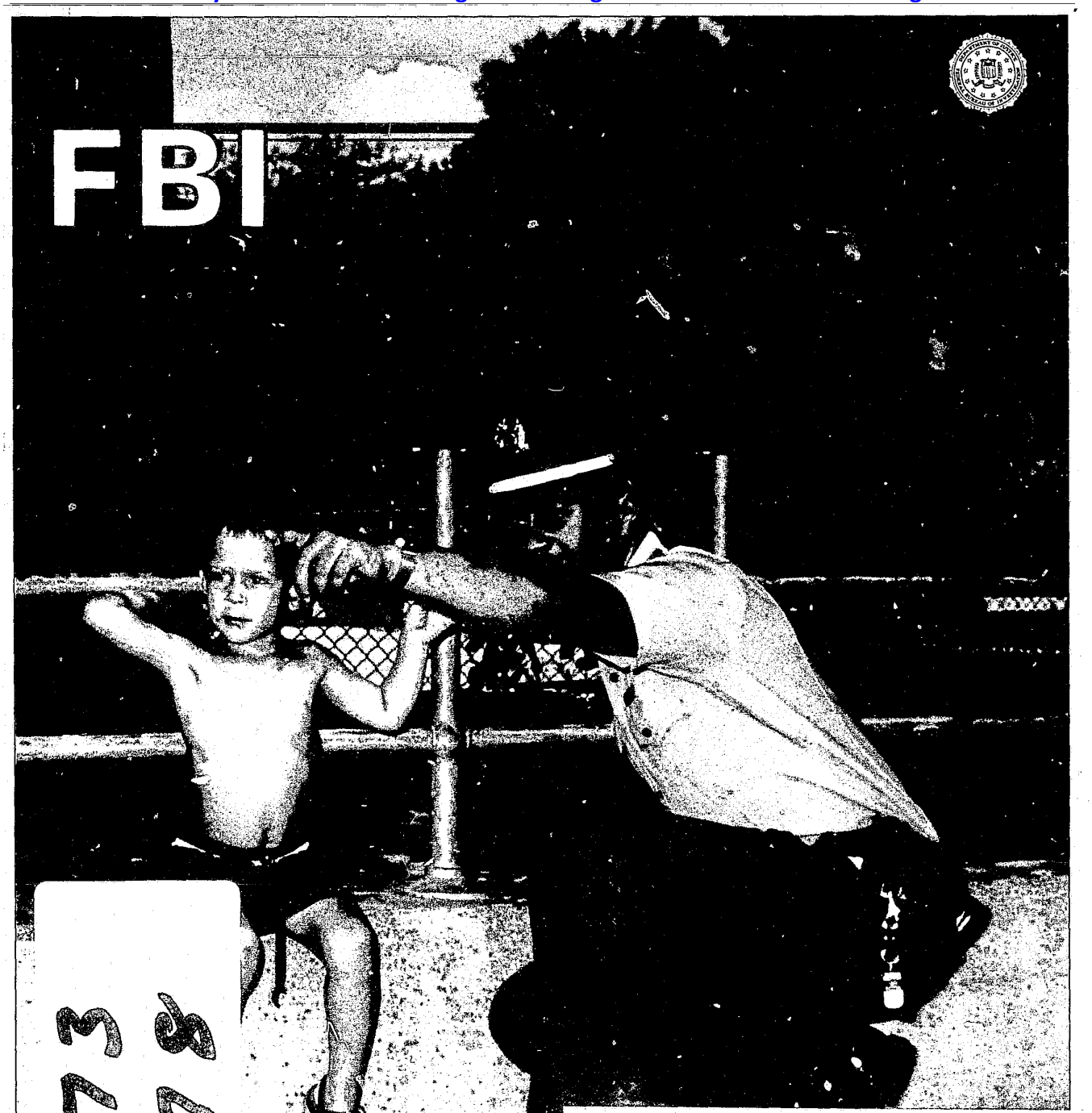


'ce Cadet Corp

Contents

March 1988, Volume 57, Number 3

FBI
Law Enforcement Bulletin

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

William S. Sessions, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs,
Milt Ahlerich, *Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Production Manager/Reprints—Mark A. Zettler

The Cover:
A police cadet gains field experience assisting a lost child (see article p. 1).

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-Class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688 USPS 383-310

110274

Executing Search Warrants in an Office Automation Environment

By
CAPT. CHARLES LUISI
Chief Investigator
DET. SGT. WALLACE R. ZEINS
Deputy Chief Investigator
and
ALAN E. BRILL
Director
Investigative Support Information Systems
Department of Investigation
New York, NY

Editor's Note: This article does not address certain legal issues associated with executing a search warrant in an office environment. Law enforcement officers preparing to execute such warrants should consult their legal adviser.

In the past, execution of a documentary search warrant was a fairly straightforward business. Once the warrant was presented, you set about examining all documents that you could find, searching for those covered by the warrant, which you would log and seize.

Today, most business organizations, even the smallest, have either memory typewriters or computer word processors. In today's technological environment, officers executing a warrant are faced with a series of challenges.[1] Does the search site contain computers or memory typewriters which could contain evidence? Does your warrant authorize you to search computer files or typewriter electronic memories? With memory typewriters, word processing programs, and personal computers, do you know how to read the memory, which may be in the form of tapes, disks, memory cartridges, or built permanently into the machine?

Identifying Office Automation

Before executing a search warrant, it is important to determine whether the site has computers or word processing memory typewriters. Computers range in size from room-sized mainframes to small, desktop personal computers. With their screens and printers, they are generally quite recognizable. However, there are small, laptop machines which can easily be concealed. Such small machines can store vast amounts of data.

The memory typewriter is frequently much more difficult to identify. While some have full TV-type screens, others have only a small display screen of one line and 10-40 characters. Still others have no special display and appear to be regular typewriters. Considering today's technological environment, it is wise to assume that all

Captain Luisi

Sergeant Zeins

typewriters have memory capabilities until it has been established on an individual basis that they do not. Therefore, to avoid intentional erasures of evidence, prohibit personnel at the search site from using any typewriter until the machine has been specifically cleared.

When examining a machine to determine whether it has memory features, first ask the operators if the machine can store documents or look at the labels. If it mentions the word "memory" or "word processor," it will have to be electronically searched. Next, determine whether there are removable storage devices. Look for slots where disks can be inserted and removed from the machine or memory cartridges that can hold hundreds of pages in an electronic memory chip. Some earlier-dated equipment store data on magnetic cards or tape cartridges. If the machine accepts any form of tape or disk, it has memory capabilities and must be searched.

On machines where there are no removable memory devices, carefully examine the keyboard for keys marked "store," "read," "write," "recall," "index," or any other similar markings. A key labeled "code" indicates that there are functions that can be called by pressing the code key either before or at the same time as another key. The code key is sometimes labeled "control" or "ctrl." On some older IBM memory typewriters, there is a control wheel adjacent to the keyboard with memory area numbers from 1 to 50 marked on it. When a machine has these keys or dials, it indicates that the machine has the capability of storing data within the machine itself. In such cases, avoid unplugging the machine at any time, as it is possible that some of the memory may be volatile and be lost if power is interrupted.

Because of difficulties associated with having to search unfamiliar equipment, it is important to obtain, if possible, a general description of the office automation equipment in use at the location to be searched. If a manufacturer and/or model number can be obtained, this obviously allows the search team to plan accordingly.

Of course, this is simply an extension of the intelligence gathering that always preceeds the successful execution of a warrant. In the case of office automation, this knowledge can be the difference between finding evidence or missing it completely. After all, those at the search site are not required to assist in the search. And instruction books, which are rarely found (once the operator understands the machine, the instructions are generally lost), are not particularly useful.

Realistically, it is practically impossible to become completely familiar with any piece of equipment in a short period of time from an instruction book. Remember that those who have information to conceal can use computers and business machines to their advantage. It is easy to hide completely the existence of a sensitive file from detection by the normal means described in instruction manuals.

Your list of intelligence gathering requirements, therefore, should include the following questions:

—Are there computers or word processors at the search site?

—If so, what brand and/or model?

—Are the machines used for word processing, data management, or financial analysis?

Director Brill

—What programs are used? If this can be determined, seek a person qualified in the use of the program to assist in the search.

—How sophisticated is the target organization in the use of their equipment? Sophisticated users can employ advanced techniques to hide data files.

Conforming Warrants to Technology

When defining the scope of the search warrant, it is important to include provisions authorizing the operation and search of automated systems. The language should authorize law enforcement officers to use the services of experts, as required. The warrant should also include authorization to search both the machine's memory and its machine-readable files. The following language was used in a recent warrant executed for a U.S. attorney in the Eastern District of New York.

"As some or all of the above described records may be stored by means of a computerized information system, the items and materials to be searched shall include the following equipment components: central processing unit, printers, terminals (keyboards and display screens), magnetic tape drives, and magnetic disk drives; and storage media: magnetic tapes, magnetic disks, punched cards, paper tapes, and computer printouts. The Deputy United States Marshals conducting this search are authorized to utilize the services of computer experts, who may not be federal law enforcement officers, in order to use and operate the computer terminals at the above specified location for the purpose of retrieving the above specified computerized record information during the course of the above authorized search, provided that such experts operate under the direction, supervision, and control of the Deputy United States Marshals."

Recent changes in technology warrant a recommendation that this wording be expanded to include optical disk drives and optical disk storage media. Devices using laser technology are scheduled for wide use within the next year and will permit storage of up to one gigabyte (1,000 million characters) on a single 5¼-inch diameter optical disk. New devices also permit paper files to be replaced by video disks, each of which can store 100,000 or more document images.

Conducting Automation Searches

A technically qualified staff, proper supplies, and a plan of action are needed to conduct a search. As noted above, there are hundreds of combinations and permutations of hardware and software in use. Your ability to properly execute the search warrant depends on your ability to locate people that can search the office automation equipment. There are several sources.

Your department may use computers or office automation and those involved in the development or use of these systems, even if they are administrative rather than sworn personnel, are the first place to look for help. Identify those who have knowledge of or experience with computers. (A growing number of sworn personnel have home computers and routinely use word processing and data management programs in their investigations.) In larger departments, more permanent arrangements can be made. At the New York City Department of Investigation,

"...the degree to which you obtain the evidence you are seeking will depend in large part on your ability to search computer-based information storage and processing systems."

the Investigative Support Information Systems Unit, which develops in-house systems, provides the technical support for searches of automated offices.

Look to other government entities for assistance. While the police function may not have an in-house staff of technical experts, another agency may. In a cooperative local/State/Federal investigation, one law enforcement organization may well be able to support the other with a technical staff.

Many departments have established a working relationship with the computer stores where they purchase their equipment. In some cases, it may be possible to gain the cooperation of the store's technical staff for assistance.

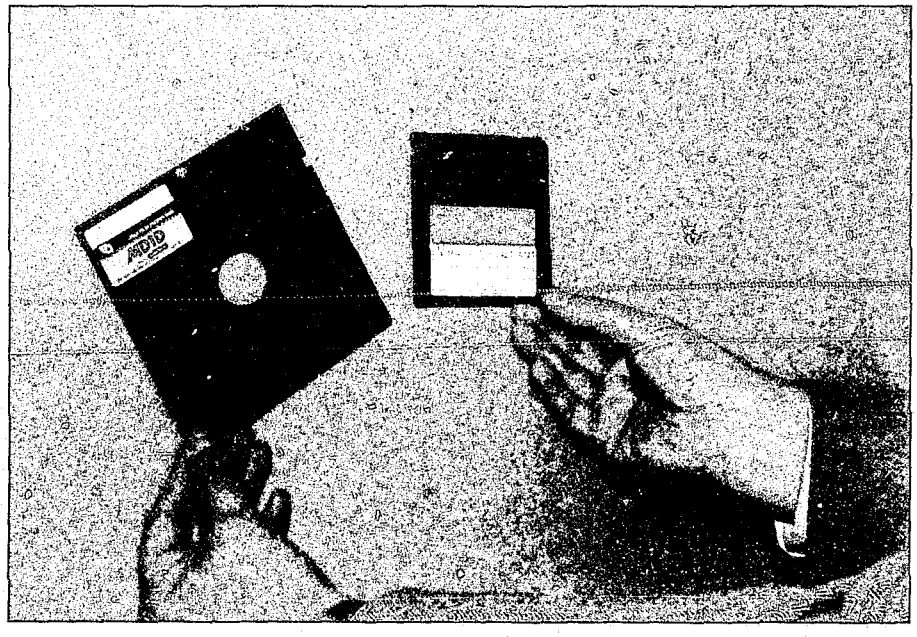
Determine whether there are consultants who could assist on an "as needed" basis. While many require payment of fees, some—particularly larger firms—may provide the service on a *pro bono* basis.

Once the staffing for the search is determined, supplies become important. While it is possible to seize small business machines, others are too cumbersome. And the cost of safeguarding a large machine for a long period when it must be left on site may be excessive. Therefore, take along on the search everything needed to operate the computer successfully and produce any evidence contained therein, e.g., blank computer printout paper, blank disks or tapes to copy files, and appropriate software. We routinely bring along programs that will enable us to copy files, examine them, and even remedy cases in which search targets suddenly erase files from their disks when the warrant is first executed. We can, in most cases, actually "unerase" the files using low-cost software.

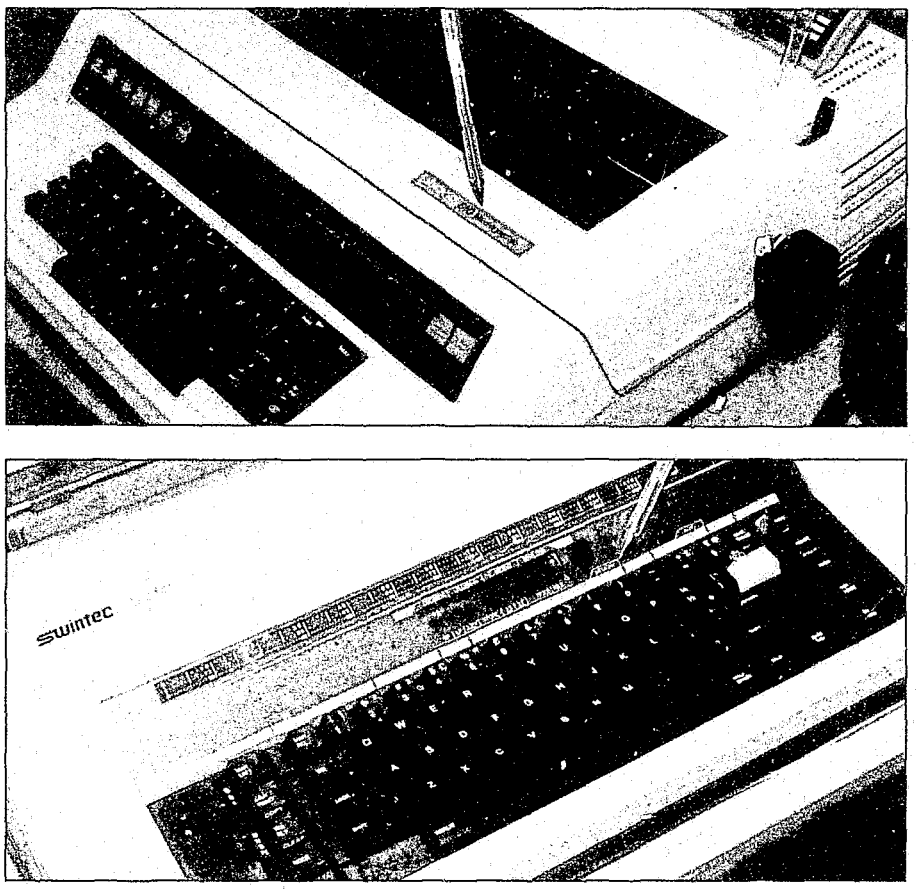
This brings up a vital point. It is very easy to destroy computerized records. On most computers, typing a simple command is all that is needed to blank out millions of characters of disk storage within seconds. Therefore, as a matter of policy, immediately take steps to move personnel at the search site away from all business machines, including typewriters, when the search warrant is executed. In these cases, seconds literally count.

Procedurally, the search of a machine is no different than a search of a file cabinet. It should be done by a team of two persons, a "searcher" and a "recorder." Begin by making an inventory of the storage media, identifying those disks or tapes that will have to be electronically searched. Remember that the label on a disk may not represent its true contents! Also remember that most personal computers have "hard disks" built into them that are not visible, but which hold tens of millions of characters of data. On memory typewriters, too, the storage devices may well be incorporated into the basic structure of the machine and not be a separate device.

For each disk or tape (including built-in disks or memory devices), proceed to identify the files stored. This may be done through the use of word or file processing software or by the use of the computer's built-in directory



These magnetic disks can store up to 1 million characters of text or the equivalent of 400 pages.



When examining a machine, look for indications of a memory capability.

search commands. Sophisticated users can easily hide files so that the names of selected files will not show up on normal directory listings. Consider the use of special software to identify these hidden files.

Examine each file on the screen to determine whether it falls within the bounds of the warrant. Consult with the prosecutor to determine whether, should you find relevant material, to seize the original files (which in many cases require seizing the entire machine that may contain volumes of material that are beyond the scope of the search warrant), or simply print out the file and mark it appropriately. In the case of large data base files, the appropriate option might be to produce a copy on your own magnetic disks. Of course, the copying process would have to be fully controlled and documented to assure that the copy was faithful to the original file in all respects. The specific evidentiary requirements for computer files and computer-produced data are beyond the scope of this article and differ by jurisdiction. However, these requirements should be included in the planning.

Conclusion

Computerized records represent the most significant challenge to those executing a documentary search warrant. As technology evolves, more and more businesses, individuals, and governmental bodies will have increasingly sophisticated office automation systems. Clearly, the degree to which you obtain the evidence you are seeking will depend in large part on your ability to search computer-based information storage and processing systems.

FBI

Footnote

John Gales Sauls, "Raiding the Computer Room: Fourth Amendment Considerations," *FBI Law Enforcement Bulletin*, vol. 55, No. 5 (Part 1) May 1986, p. 25; No. 6 (Conclusion) June 1986, p. 24.