

Copyright 1995 Kenneth Rosenblatt.
All rights reserved.

You may find this document easier to read if you import it into your own word processor program and format it with a proportional spaced font (e.g., CG Times, Times Roman).

SAMPLE AFFIDAVIT FOR SEARCH WARRANT TO SEARCH
SUSPECTED CRACKER'S RESIDENCE

SUPERIOR COURT OF CALIFORNIA
SANTA CLARA COUNTY JUDICIAL DISTRICT

STATE OF CALIFORNIA
COUNTY OF SANTA CLARA

AFFIDAVIT IN SUPPORT
OF SEARCH WARRANT

Personally appeared before me this ___ day of *, 1988, Detective Jane Doe of the Palo Alto Police Department, who on oath makes complaint, and deposes and says that she has and there is just, probable, and reasonable cause to believe and that she does believe there is certain personal property now located at

1111 Able Street, in the City of Palo Alto, County of Santa Clara, State of California, that property:

- (X) Stolen or embezzled;
- (X) Used as the means of committing a felony;
- (X) In the possession of a person with the intent to use same as a means of committing a public offense, or in the possession of another to whom he/she may have delivered same for the purpose of concealing or preventing its discovery;
- (X) Constituting evidence tending to show that a felony has been committed or that a particular person has committed a felony.

DESCRIPTION OF PLACES TO BE SEARCHED

The premises of 1111 Able Street are further described as follows:

A single-story house, brown in color with yellow trim, with the numbers "1111" on a mailbox at the front of the house and next to the front door. The nearest cross-street is Baker Street.

The premises to be searched also include any and all yards, outbuildings, storage areas, garages, carports, sheds, or mailboxes assigned to the described premises, including but not limited to those listed above.

DESCRIPTION OF PROPERTY TO BE SEARCHED/SEIZED

The following personal property has been grouped into categories for clarity. Each category contains a group of personal property, information, and other items to be searched/seized, regardless of the media which they appear in or on.

The term "media" encompasses all "writings," as that term is defined by section 250 of the California Evidence Code, and documents and records, magnetic media (e.g., floppy disks, hard disks, cassette tapes, magnetic tapes, removable media, tape and/or data cartridges), photographic media (e.g., film, microfilm, photocopies, faxes), optical media (e.g., CD-ROMs), and all information stored within a computer or computer peripheral in any form.

The personal property and other items to be searched/seized are described as follows:

1. All media containing the telephone number 408-xxx-xxx1.
2. All media containing the word "actor."
3. All media containing the word "pilot."
4. All media referring to the name Jared Smith.
5. All media referring to the name Lisa Jones.
6. All media referring to VICTIM.
7. All media containing the phrase "Bishop One."
8. VICTIM's database software.
9. All media containing the following words or phrases [WHICH IN THE COMPLETE AFFIDAVIT IS ACCOMPANIED BY A LIST OF FILE NAMES included within the victim's software].

10. Computer systems, computer hardware (including peripherals and cables), software, and data, including, but not limited to, central processing units (CPUs), hard disk drives, floppy disk drives, tape drives, removable media drives, optical/CD-ROM drives, servers, workstations, display screens, input devices (including but not limited to keyboards, mice, and trackballs), printers, modems, peripherals, floppy disks, magnetic tapes, cassette tapes, removable storage media (such as Bernoulli media), and/or optical/CD-ROM disks or cartridges, found together or separately from one another.

11. Documentation or other material describing the operation of any computer systems, computer hardware, software, and/or computer peripherals found at the premises, including instructions on how to access disks, files, or other material stored within same, including but not limited to computer manuals, printouts, passwords, filename lists, "readme" and/or "help files", as well as any documentation describing how to access or use a bulletin board.

12. Devices commonly known as "blue boxes", and/or any electronic devices used to circumvent or bypass phone companies' billing systems;

13. Any and all materials reflecting, recording, or advertizing to computer access codes (including but not limited to lists of computer accounts, passwords, and access codes for any computer, computer system, or computer network).

14. Any and all computer printouts, notebooks, papers, bills, or other materials reflecting, recording, or advertizing to telephone numbers (with the exception of published telephone books, but excluding notations added to same), credit card numbers, and/or telephone access card numbers.

15. Any and all receipts, charge slips, carbons, names, numbers, addresses, memoranda, or notations pertaining to the use of credit cards or telephone access numbers.

16. Any and all receipts, charge slips, carbons, names, numbers, addresses, memoranda or notations pertaining to merchandise mail or telephone orders, or orders for computer supplies.

17. Any and all materials reflecting, recording, or advertizing to names, locations, phone numbers, and passwords for computer bulletin boards, including the names of users of said boards.

18. Any and all telephones capable of storing and/or automatically dialing pre-programmed phone numbers, including numbers stored as part of an "automatic dialing feature."

19. Evidence of identity, use, or ownership of all of the items/information specified above.

20. Evidence of occupancy and control of said premises, including but not limited to, utility company bills, cancelled mail envelopes, personal identification papers, photographs, rent receipts, and keys.

STATEMENT OF PROBABLE CAUSE

I, Detective Jane Doe, declare that the facts in support of issuance of this search warrant and court order are as follows:

I am a detective employed by the Palo Alto Police Department in Santa Clara County, California. [THE DETECTIVE HAD LITTLE HIGH-TECH EXPERTISE.]

I am currently investigating an apparent series of computer crimes, including trespass by telephone, perpetrated against the business operating under the name of [VICTIM].

During the course of this investigation, I obtained a search warrant authorizing the installation of a trap and trace on a phone line connected the computer owned by [VICTIM] which was being illegally accessed by persons unknown. A true and correct copy of the affidavit in support of that warrant is attached hereto and incorporated by reference herein as Exhibit 1 to this affidavit. Exhibit 1 provides details of the intrusion and my investigation to that date.

The results of the trap and trace authorized by that warrant, when matched with computer logs maintained by the [VICTIM] recording when that computer had been accessed, revealed that the intruder was calling from a telephone registered to SUSPECT at 1111 Able Street. The trap recorded five separate intrusions: one each on July 30, August 1, August 2, August 5, and August 8 of 1988. The computer log indicated that each of those intrusions lasted for several hours, and recorded the intruder copying portions of [VICTIM]'s proprietary source code.

On August 1, I obtained a search warrant authorizing installation of a pen register on the telephone registered to SUSPECT at 1111 Able Street. A true and correct copy of the affidavit in support of that warrant is attached hereto and incorporated by reference herein as Exhibit 2 to this affidavit. The results from the pen register confirmed that someone at 1111 Able Street was using that telephone to illegally access and download [VICTIM]'s proprietary software from [VICTIM]'s computer.

I have checked Department of Motor Vehicle records, which indicate that SUSPECT, a male with a DOB of 10/15/69, lists 1111 Able Street as his residence address. [REQUEST TO SEARCH AUTOMOBILE AND ACCOMPANYING JUSTIFICATION IS OMITTED]. I drove by 1111 Able Street yesterday and confirmed that the property description listed above for those premises is correct.

Ms. Vic Rep confirms that SUSPECT does not work for [VICTIM], has no apparent connection with the company, and has never had permission to access [VICTIM]'s computers.

Ms. Vic Rep has also related the following details of the intrusions which bear on evidence likely to be found at SUSPECT's residence. As discussed in

previous warrants, SUSPECT accessed [VICTIM]'s computer by dialing into the line with the number 408-xxx- xxx1. SUSPECT has accessed the accounts of two [VICTIM] employees: Jared Smith and Lisa Jones.

Jared Smith's password is "actor"; Lisa Jones' password is "pilot." The computer is referred to by a specific name, "Bishop One" (much as buildings can bear different alphabetic or numeric designations, [VICTIM] has named its computers to distinguish them from one another). When accessing the computer, the name "Bishop One" appears on the screen, and may also appear on files copied by an intruder from that computer. I suspect that the SUSPECT has also recorded the names and passwords of the legitimate users of the accounts he penetrated.

[VICTIM]'s proprietary database software is called LEGION. LEGION, like most sophisticated software, contains numerous files, each of which in turn contains instructions and data. When someone uses a computer to copy software, that person copies the files making up that software. Unless that individual goes to the trouble of changing the names of the files, those "filenames" will still be found in the copied software, and can be located. Attached hereto and incorporated by reference herein as Exhibit 3 to this affidavit is a list of a portion of the filenames for the LEGION software.

I now seek a search warrant to search the premises described above for the property described above.

From my training and experience, I am aware that thieves will often hide stolen property in yards, outbuildings, storage areas, garages, carports, or sheds.

[AUTOMOBILE JUSTIFICATION OMITTED.]

Justification for seizing property described above:

Request to seize computers, peripherals, and loose media:

Computers:

As stated in the previous warrants obtained during this investigation, the intruder (now identified as SUSPECT) has been using a computer to access [VICTIM]'s computer from the premises to be searched. From my training and experience, and my conversations with Sgt. A.K. Jones, I know that a computer which has been used to access another computer without authorization is likely to contain evidence of that intrusion.

For example, the intruder's computer is likely to contain software, passwords, and access codes used to access [VICTIM]'s computer. It will also contain any data stolen from [VICTIM]'s computer; intruders also frequently store such data on floppy disks located at the same premises.

Moreover, in addition to containing evidence, the computer is an instrumentality of the offense.

I have been advised by Sgt. A. K. Jones, and I know from my training and expertise, that computer systems commonly consist of computer hardware,

software, and data, including central processing units (CPUs), hard disk drives, floppy disk drives, tape drives, removable media drives, optical/CD-ROM drives, servers, workstations, display screens, input devices (including but not limited to keyboards, mice, and trackballs), printers, modems, peripherals, floppy disks, magnetic tapes, cassette tapes, removable storage media (such as Bernoulli media), and/or optical/CD-ROM disks or cartridges, found together or separately from one another. More powerful computer systems may include multiple computers connected together, including workstations and servers.

Items related to computer intrusion activities in general:

In considering the request to search/seize the property described above, and in particular items #12-19, I request that this Court consider that SUSPECT appears to fit the profile of a cracker described below.

The cracker profile:

I know each and every fact stated below based on my previously described training and expertise, and from speaking with Palo Alto Police Department Sgt. A.K. Jones. Sgt. Jones has investigated computer crime for five years. He has investigated twenty incidents of computer intrusion, has received training in computer forensics from a nationally recognized computer training organization, and has attended numerous high-technology crime training seminars where he received training in the investigation of computer intrusion. Sgt. Jones has examined the facts of this case, and agrees that SUSPECT appears to match the profile of a cracker. [NOTE THAT SGT. JONES IS NOW A WITNESS.]

According to Sgt. Jones, persons who engage in the unauthorized access and use of computer systems are known as "crackers." (The more commonly used term, "hacker," also includes innocent computer users who enjoy programming computers.) Crackers usually use their own computer systems to engage in the unauthorized access and use of computer systems.

Crackers' computer systems commonly consist of computer systems, computer hardware (including peripherals and cables), software, and data, including, but not limited to, central processing units (CPUs), hard disk drives, floppy disk drives, tape drives, removable media drives, optical/CD-ROM drives, servers, workstations, display screens, input devices (including but not limited to keyboards, mice, and trackballs), printers, modems, peripherals, floppy disks, magnetic tapes, cassette tapes, removable storage media (such as Bernoulli media), and/or optical/CD-ROM disks or cartridges, found together or separately from one another. Such systems also commonly include electronic cables linking computer systems to other systems or phone lines.

Crackers usually break into computers to: (1) explore computer systems to learn how they operate and to view information stored on those computer systems; (2) vandalize, or otherwise interfere with the operation of those computers; (3) steal information (including software) located on those computers for their own use; (4) obtain credit information and/or financial records of other individuals or entities; (5) use said information to purchase goods and services; and/or (6) avoid paying the legitimate telephone service or toll charges necessary to access other computers.

Crackers usually store certain information on their computers. For example, the typical cracker will possess passwords and access codes used to

gain entry to other computers. Crackers will also often maintain credit card numbers obtained from intrusions by the cracker, or others, into computer systems containing credit information (such as computers maintained by credit information services). Crackers will also often possess telephone access numbers used to make free phone calls. (Since many of the techniques used to break into computer systems require repeated phone calls, such crackers have an incentive to discover access codes which will allow them to make free phone calls. One such technique is to steal access codes for cellular telephones by using a scanner which can intercept the signals transmitting billing information from the phone to a switching station.)

Telephone access codes are like credit card numbers. Phone companies provide such numbers to their subscribers to allow them to place toll calls from any location and have those calls automatically billed to their account. For example, a person charging a phone call to his or her Pacific Bell Telephone credit card number is using a telephone access code. The call then appears on that person's monthly phone bill.

Many crackers communicate with other similarly inclined individuals electronically, by using "bulletin boards." A computer bulletin board can be thought of as an electronically generated means of communication between computer users, in which each party to the communication can either send or receive information through their respective computers with the use of a modem. (A modem allows a computer to communicate with another computer over telephone lines.) A person typically operates a bulletin board on one "host" computer. Users of the board call into that computer and leave messages or participate in joint activities on that computer.

There are thousands of bulletin boards across the United States today. The vast majority of bulletin boards are legitimate. However, I am aware that there are many "pirate" bulletin boards used primarily to communicate information on how to illegally access computers and steal information from those computers.

Crackers will commonly use bulletin boards to exchange telephone access codes with similarly inclined individuals. They will also use those boards to exchange information on how to illegally access computers, including the account numbers and passwords for those systems. They will also exchange software used to break into computers (such software seeks to "guess" passwords and access codes by generating numerous letters and numbers). They will also exchange software designed to find, record, or capture telephone access codes. (Such software uses a similar technique to "guess" the access codes.)

Crackers use this information to purchase goods and services (e.g., by using illegally obtained credit information). Many crackers call in those orders to mail order merchandisers, particularly computer stores, to purchase various items. The advantage to such a technique is that the cracker need not present an actual credit card, but only the credit card number.

Thus, the computers used by crackers will often contain such information. Such information found on SUSPECT's computer or premises will be evidence of SUSPECT's intent in accessing [VICTIM]'s computer.

In addition to software used to guess telephone access codes, there are mechanical devices used to circumvent the billing systems used by telephone companies. One example is a "blue box." Such devices, and others known by similar names which work in similar ways, send signals through phone lines which

"fool" the telephone companies' computers into allowing the caller to avoid paying for the call.

Crackers often keep documentation of their use of telephone access codes and credit card numbers. Persons illegally accessing computers or computer networks also keep records of account numbers and passwords used to break into those computers. Such documentation may consist of scraps of paper, note pads, or typewritten lists, or may be maintained within the cracker's computer itself. Sometimes crackers will add this information to the computer printouts or computer manuals which set forth procedures used to operate their computer and/or software. Sometimes crackers will add this information to written instructions supplied with the "illicit" software described above. Finally, this information may consist of materials containing instructions on how to unlawfully obtain access codes or access computers.

Any and all of the information discussed above may be kept on magnetic or optical media located within the cracker's computer, or on magnetic media secreted somewhere else. In addition to the information discussed above, such persons may also collect a great deal of stolen software on disks or other magnetic or optical media.

Items relating to the cracker profile:

SUSPECT appears to fit the profile of a cracker, as he has invaded [VICTIM]'s computer without authorization, and has copied/stolen software for that computer. He is not an employee; he appears to have chosen this computer at random. There is no reason to believe that he has only invaded this computer system.

Given that the intruder appears to fit the profile of a cracker, I expect to find at the premises to be searched, and seek permission to search for, the following items: telephone access codes; telephone numbers belonging to other computers; computer access codes; information pertaining to bulletin boards (including telephone numbers for same); credit card numbers; and records of mail order and other transactions. I also seek permission to search for and seize telephone bills and credit card receipts.

I believe that such information will yield evidence of: stolen telephone access codes; intrusion into other computer systems; conspiracy with other patrons of bulletin boards to share access codes and stolen software; and credit card fraud.

I expect to find this information within the computer, on loose magnetic media (e.g., floppy disks), and in documentary form. I also expect to find telephones capable of dialing pre-programmed phone numbers (containing the phone numbers of confederates).

Indicia of occupancy:

Based on my training and experience, I know that occupants of dwellings usually receive correspondence addressed to the occupants at that particular dwelling. Such correspondence usually includes, but is not limited to, phone bills, utility bills, rental agreements, rent receipts, identification papers, cancelled mail envelopes, and personal letters. Additionally, I know that other evidence of ownership and control of said dwellings can usually be found on the

occupants of said dwellings and may include, but is not limited to keys, rent receipts and photographic identification documents, with names and addresses on them.

Permission to be accompanied by an expert for the purpose of examining and operating computers found at the premises:

I am not a computer expert, and I will need expert assistance to competently examine and seize computer hardware and software.

Vic Rep. is a computer expert familiar with both the hardware and software environments which are likely to be encountered in the execution of the search warrant, and with the methods for safely extracting or copying data (evidence) from such systems. She is also competent to identify the LEGION software, and I request permission to have her assist me in that endeavor. She has consented to be ordered to assist in this search.

I ask this court to order Vic Rep. to accompany me to assist in searching any computers found at any of the premises to be searched, and identifying the LEGION software and any other [VICTIM] property found at the premises.

Permission to remove computers and loose media for examination off-site:

I know the following facts based on my experience (and/or) from discussions with Sgt. A. K. Jones.

I believe that some of the information sought to be searched/seized may be contained on computers and/or separate (or "loose") "computer media" (e.g., floppy disks, Bernoulli, floptical, or other removable storage media, CD-ROM disks, cartridges, or tapes). Searching SUSPECT's computer and separate computer media to the degree necessary to discover all information stored within that computer or media which is encompassed by the warrant in this case would be difficult and would risk destruction of evidence. I therefore request permission to remove all computers and computer media for further examination.

It would be difficult to perform a thorough search of the SUSPECT's computer at the scene because I may not be familiar with the operating system used on that computer. I will need an expert to perform that search, and I may need different experts depending upon the type of computer found at the premises.

Furthermore, a search performed at the premises could risk destruction of evidence. Persons concerned about detection are able to "rig" their computers in such a way that an otherwise innocuous instruction acts as a signal for the computer to erase data. This is particularly true of "crackers," who are more likely to possess the necessary skills than are most criminals using computers.

I may not be able to perform even a cursory search without spending a great deal of time at the scene ensuring that the computer has not been "rigged." Those persons may also employ computer security programs which can only be bypassed, if they can be circumvented at all, by specialists using a sophisticated laboratory.

Computers are capable of storing large amounts of data; a thorough search of a single computer may take days or weeks. It would be impractical to perform such a search at the premises.

It would also be difficult to search all loose computer media at the scene. SUSPECT may maintain too many disks to allow a thorough search within a reasonable time. Some removable storage media (such as Bernoulli media) may contain the equivalent of tens of thousands of pages of information. (I cannot exclude even those floppy disks labeled as commercial software, because it is easy for anyone to copy over new information onto those media.)

It is impossible to know how many floppy disks are at the premises until I arrive. In addition, in order to avoid using SUSPECT's computer (which may be rigged) to examine those loose computer media, I would have to bring another computer onto the premises. It is impossible to predict which application programs (as well as other programs, such as drivers) out of the hundreds available have been used by SUSPECT to create files stored on the computer media. Therefore, it is impossible to ensure that any computer brought onto the premises could be used to examine the media. Thus, I request permission to remove those media for further examination.

Permission to seize computer peripherals:

As discussed above, I am requesting permission to search and seize computer systems, computer hardware, software, and data located at the premises. I intend to search and seize computer equipment which could be considered to be computer peripherals, including but not limited to display screens (monitors), keyboards, input devices (such as mice and trackballs), printers, tape drives, optical/CD-ROM drives, modems (used to communicate with other computers), found together or separately from one another.

I need to seize monitors, keyboards, input devices, and printers because they are integral parts of computer systems and are used to completely perform the functions of those computer systems, including the display of data (potential evidence) contained within those systems. They are also instrumentalities of the illegal accesses accomplished by SUSPECT.

Moreover, in order to ensure accurate retrieval of the evidence contained within the computer, I need to be able to seize and analyze the computer in its current configuration. I need to seize modems because they may contain evidence (in the form of stored phone numbers) of other computers with whom the intruder communicated. Moreover, the modem is evidence that SUSPECT was able to dial into [VICTIM]'s computer, and is an instrumentality of the offense.

Permission to seize documentation:

I also request permission to seize any documentation or other material describing the operation of any computer, software, and/or computer peripherals found at the premises, including instructions on how to access disks, files, or other material stored within same, including but not limited to computer manuals, printouts, passwords, file name lists, "readme" and/or "help files." That information may be necessary to enable me to operate computers and software searched and/or seized in accordance with the warrant requested by this affidavit. That documentation is also relevant insofar as it may contain information identifying the owner and/or user of that computer, and provide evidence that the owner of the computer knew how to use the computer containing relevant information.

Permission to videotape:

I seek permission to videotape the execution of this warrant. I expect to examine computers at the scene of the search. Those computers may be operating when I arrive at the premises. The images on the screens of the computers are transient (they disappear when the computer is turned off). I need to be able to videotape any such images because they may be evidence (e.g., incriminating documents being written by the user when the warrant is executed). Furthermore, I want to videotape the examination of those computers to ensure that there is a record of the steps taken during that examination. Should there be a question concerning the procedures employed in obtaining evidence from those computers, the videotape may be useful in documenting what was done.

Therefore, your affiant believes that evidence of the commission of felony violations of California Penal Code section 484 (theft) and 502 (computer intrusion) will be found upon the premises and in the records heretofore described.

That based upon the above facts, your affiant prays that a search warrant be issued with respect to the above location for the seizure of said property, and that the same be held under Penal Code section 1536 and disposed of according to law.

AFFIANT

Subscribed and sworn to before me
this ___ day of August 1988.

JUDGE OF THE SUPERIOR COURT