IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF:
xxx xxxxx xxxxx xxxxx
xxxxx xxxxxx, Missouri
Single Family Residence,
located within the Western District of Missouri

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

COMES NOW Special Agent xxxxxxxxxxx xxxxxx of the United States Department of Education (hereinafter, ED), Office of Inspector General (hereinafter, OIG), who is currently assigned to the Computer Crimes Investigation Division (hereinafter, CCID), being of lawful age and first duly sworn upon my oath, to depose and state as follows:

INTRODUCTION

I have been a Special Agent of the ED-OIG for approximately xxxx and a xxxx years. I am assigned to the investigation of white-collar crimes involving ED programs and resources, and in particular to the investigation of crimes involving computer fraud, abuse, and network intrusions. For approximately the last three years, I had the additional part-time duty of participating as a forensic field examiner for the ED-OIG Computer Analysis Team, which specializes in searching for and analyzing evidence stored on computers. I am currently assigned to the ED-OIG-CCID as a full time computer crime investigator.

During my career as a Special Agent, I have participated in several investigations involving computer-related offenses, and have participated in the execution of several search warrants involving the searches and seizures of computers, computer equipment, software, and electronically stored information. I have personally submitted affidavits in connection with approximately three searches in computer-crime cases. I have interviewed numerous persons involved in the unlawful use of computers to commit fraud against ED programs, and have analyzed computer hardware and software recovered during the execution of search warrants. Additionally, I have received both formal and informal training in the field of computers and network intrusions from the Federal Law Enforcement Training Center, ASR Data Forensics, Guidance Software, and various forensic and network intrusion training providers.

This affidavit seeks the issuance of a search warrant for the residence of xxxxxx xxxxxxxx (hereinafter, the SUBJECT), who is the target of an investigation currently being conducted by ED-OIG-CCID. As set forth in more detail below, there is probable cause to believe the SUBJECT has committed and is continuing to commit criminal unauthorized access into xxxx xxxxxxxx xxxxxxx xxxxxxx (hereinafter, xxxxx), in violation of 18 U.S.C. § 1030, and that the SUBJECT has committed and is continuing to commit illegal interceptions of electronic communications through the use of a keystroke monitoring program in violation of 18 U.S.C. § 2511, and that he maintains at his residence computers, electronic equipment, software programs, storage media, records, and other evidence and instrumentalities of his criminal activities as described more fully herein.

DEFINITIONS

I am familiar with the following terms from my training and experience, which are relevant to this Affidavit and Application:

Addresses = Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. Other addresses include Uniform Resource Locater (URL) addresses, such as “http://www.usdoj.gov,” which are typically used to access web sites or other services on remote devices. Domain names, host names, and machine addresses are other types of addresses associated with Internet use.

Citrix = A web-based, remote access system, which provides the user a secure way to access their agency's server from a remote location, at anytime, using any computer, which has the Citrix client installed, over an Internet connection.

Domain = A group of Internet devices that are owned or operated by a specific individual, group, or organization. Devices within a domain have IP addresses within a certain range of numbers, and are usually administered according to the same set of rules and procedures.

Domain Name = Identifies a computer or group of computers on the Internet, and corresponds to one or more IP addresses within a particular range. Domain names are typically strings of alphanumeric characters, with each "level" of the domain delimited by a period (e.g., Computer.networklevel1.networklevel2.computer). A domain

name can provide information about the organization, ISP, and physical location of a particular network user.
Unauthorized Access = The gaining of access to a computer, without or in excess of authority, to obtain information. Access can be achieved by simply stealing or guessing a user's password, or a detailed program can be created to allow the intruder to gain access.
Internet = A global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links, and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
Internet Service Providers ("ISPs") = Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide
Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it.
IP Address = The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses.
Keystroke Monitoring = A process whereby a computer system users and/or administrators can view or record both the keystrokes entered by a computer user and the computer's response during a computer session. Examples of keystroke monitoring would include viewing characters as they are typed by users, reading users' electronic mail, and viewing other recorded information typed by users. Some keystroke monitoring software programs store the keystrokes in a log file.
Log File = Computer files that contain records about system events and status, the activities of users, and anomalous or unauthorized computer usage. Names for various log files include, but are not limited to: user logs, access logs, audit logs, transactional logs, and apache logs.
Server = A centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large agency, such as ED, it is common for individual employees to have client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (and even thousands) of miles away from the client computers.
User Name or User ID = Most services offered on the Internet assign users a name or ID, which is a pseudonym that computer systems use to keep track of users. User names and IDs are typically associated with additional user information or resources, such as a user account protected by a password, personal or financial information about the user, a directory of files, or an email address.

USE OF COMPUTERS TO CONDUCT CRIMINAL ACTIVITIES

In pertinent part, Title 18, United States Code, Section 1030 prohibits the following:

> (a) Whoever - intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains – (B) information from any department or agency of the United States intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States, and such conduct affects that use by or for the Government of the United States . . . shall be punished as provided in subsection (c) of this section.

In pertinent part, Title 18, United States Code, Section 2511 prohibits the following:
Except as otherwise specifically provided in this chapter any person who –

> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, and wire, oral, or electronic communication . . . shall be punished as provided in subsection (4). . . .

•

Based on my training and experience, I am familiar with the use of computers as an instrumentality in a crime, as creating contraband, or as containing contraband. I know that computer hardware, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

I know that when an individual uses a computer to obtain unauthorized access to a server over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is "used as a means of committing [the] criminal offense" according to Rule 41(b)(3). In particular, the individual's computer is the primary means for accessing the Internet, communicating with the victim computer, and ultimately obtaining the unauthorized access that is prohibited by 18 U.S.C. § 1030. The computer is also likely to be a storage device for evidence of crime because records and evidence relating to the crimes are stored on the computers for future use. Those records and evidence may include files that recorded the unauthorized access, stolen passwords, computer logs, individual's notes as to how the access was achieved, and other records that indicate the scope of the individual's unauthorized access. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime.

In this case, the warrant application requests permission to search and seize for evidence, likely digital and paper, related to the unauthorized access into the United States Department of Education's computer network and of illegal interceptions of electronic communication. This digital and paper evidence constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware that may contain evidence of computer intrusions and/or unauthorized access and of illegal interceptions of electronic communications, if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. I believe that, in this case, the computer hardware is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

SEARCH AND ANALYSIS OF THE EVIDENCE

Based upon my knowledge, training, and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to insure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer be seized and subsequently processed by a qualified computer specialist in a laboratory setting.

This is true because computer storage devices (such as hard disks, diskettes, tapes, compact disks, thumb drives, etc.,) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take days or weeks, depending on the volume of data stored, and it could be impractical to attempt this kind of data analysis "on-site."

INCREMENTAL APPROACH TO SEIZING THE EVIDENCE

Your Affiant recognizes that the SUBJECT and his family use their computers for a wide range of day-to-day tasks, which are not the criminal activity under investigation, and that a seizure of the SUBJECT's computers may have the unintended and undesired effect of limiting the SUBJECT and his family's ability to conduct their normal day to day activities. In response to these concerns, the agents who execute the search will take an incremental approach to minimize the inconvenience to the SUBJECT's family and to minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:

A. The computer forensic examiner will attempt to create an electronic "image" of the computers, which are likely to store the data and information described in Attachment A. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. A computer forensic examiner will conduct an off-site search for the computer files described in Attachment A, from the "imaged" copy, at a later date. If the computer forensic examiner successfully images the SUBJECT's computers, the agents will not conduct any additional on-site searches or seizures of the Subject's computers.

B. If "imaging" proves impractical, or even impossible for technical reasons, then the agents will seize those components of the SUBJECT's computer system that the computer forensic examiner believes must be seized to permit the agents to locate the computer files described in Attachment A. The components will be seized and taken in to the custody of the ED-OIG-CCID. If the SUBJECT so requests, the computer forensic examiner will, to the extent practicable, attempt to provide the SUBJECT with copies of any files not within the scope of the warrant that may be necessary or important to the continuing function of the SUBJECT's or his family's legitimate business and/or their day to day activities. If, after inspecting the computers, the computer forensic examiner determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, ED-OIG-CCID will return it within a reasonable time.

DATA ANALYSIS

Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Since computer evidence is extremely vulnerable to tampering or destruction (either from external sources or from destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Searching the SUBJECT's computer system for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, a computer forensic examiner may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, a computer forensic examiner may be able to locate the materials covered in the warrant by looking for particular directory or file names.

Based on my knowledge, training, and experience, I know that, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information.

Furthermore, computer data or remnants of such data can be recovered months or even years after they have been deleted from a hard drive. When a person "deletes" a file on a personal computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten.

In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

These steps may require the computer forensic examiner to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, I request permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

CONCLUSION

xxxxxxxxxxx xxxxxx
Special Agent
United States Department of Education
Office of Inspector General
Computer Crimes Investigation Division

Subscribed and sworn before me
this ___ day of xxx 2005.

xxxxxxx xxxxxxxx
CHIEF UNITED STATES MAGISTRATE JUDGE