(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number)

B. The contents of wire or electronic communications held or maintained in **[ISP's]** computer systems on behalf of the accounts identified in Part A at any time up through and including the date of this Subpoena, EXCEPT THAT you should NOT produce any unopened incoming communications (i.e., communications in "electronic storage") less than 181 days old.

"Electronic storage" is defined in 18 U.S.C. 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials, unless they have been in "electronic storage" for more than 180 days.

[Return to Main Text]

APPENDIX F: Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers

(Appendix F updated December 2006)

This appendix provides sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of computers. The discussion focuses first on the proper way to describe the property to be seized in the warrant itself, which in turn requires consideration of the role of the computer in the offense. The discussion then turns to drafting an accompanying affidavit that establishes probable cause, describes the agent's search strategy, and addresses any additional statutory or constitutional concerns.

I. DESCRIBING THE PROPERTY TO BE SEIZED FOR THE WARRANT

The first step in drafting a warrant to search and seize computers or computer data is to describe the property to be seized for the warrant itself. This requires a particularized description of the evidence, contraband, fruits, or instrumentalities of the crime that the agents hope to obtain by conducting the search.

Whether the "property to be seized" should contain a description ofinformation (such as computer files) or physical computer hardware depends on the role of the computer in the offense. In some cases, the computer hardware is itself contraband, evidence of a crime, or a fruit orinstrumentality of a crime. In these situations, Fed. R. Crim. P. 41

expressly authorizes the seizure of the hardware, and the warrant will ordinarily request its seizure. In other cases, however, the computer hardware is merely a storage device for electronic files that are themselves contraband, evidence, or instrumentalities of crime. In these cases, the warrant should request authority to search for and seize the information itself, not the storage devices that the agents believe they must seize to recover the information. Although the agents may need to seize the storage devices for practical reasons (e.g., the electronic media cannot be imaged without first seizing the hardware), such practical considerations are best addressed in the accompanying affidavit. The "property to be seized" described in the warrant should fall within one or more of the categories listed in Rule 41(b):

(1) "property that constitutes evidence of the commission of a criminal offense"

This authorization is a broad one, covering any item that an investigator "reasonably could . . . believe" would reveal information that would aid in a particular apprehension or conviction. Andresen v. Maryland, 427 U.S. 463, 483 (1976). Cf. Warden v. Hayden, 387 U.S. 294, 307 (1967) (noting that restrictions on what evidence may be seized result mostly from the probable cause requirement). The word "property" in Rule 41(b)(1) includes both tangible and intangible property. See United States v. New York Tel. Co., 434 U.S. 159, 169 (1977) ("Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause."); United States v. Biasucci, 786 F.2d 504, 509-10 (2d Cir. 1986) (holding that the fruits of video surveillance are "property" that may be seized using a Rule 41 search warrant). Accordingly, data stored in electronic form is "property" that may properly be searched and seized using a Rule 41 warrant. See United States v. Hall, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

(2) "contraband, the fruits of crime, or things otherwise criminally possessed"

Property is contraband "when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken." Hayden, 387 U.S. at 302 (quoting Gouled v. United States, 255 U.S. 298, 309 (1921)). Common examples of items that fall within this definition include child pornography, see United States v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995), pirated software and other copyrighted materials, see United States v. Vastola, 670 F. Supp. 1244, 1273 (D.N.J. 1987), counterfeit money, narcotics, and illegal weapons. The phrase "fruits of crime" refers to property that criminals have acquired as a result of their criminal activities. Common examples include money obtained from illegal transactions, see United States v. Dornblut, 261 F.2d 949, 951 (2d Cir. 1958) (cash obtained in drug transaction), and stolen goods. See United States v. Burkeen, 350 F.2d 261, 264 (6th Cir. 1965) (currency removed from bank during bank robbery).

(3) "property designed or intended for use or which is or had been used as a means of committing a criminal offense"

Rule 41(c)(3) authorizes the search and seizure of "property designed or intended for use or which is or had been used as a means of committing a criminal offense." This language permits courts to issue warrants to search and seize instrumentalities of crime. See United States v. Farrell, 606 F.2d 1341, 1347 (D.C. Cir. 1979). Computers may serve as instrumentalities of crime in many ways. For example, Rule 41 authorizes the seizure of computer equipment as an instrumentality when a suspect uses a computer to view, acquire, and transmit images of child pornography. See Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (stating in an obscenity case that "the computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime."); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996). Similarly, a hacker's computer may be used as an instrumentality of crime, and a computer used to run an illegal Internet gambling business would also be an instrumentality of the crime.

Here are examples of how to describe property to be seized when the computer hardware is merely a storage container f or electronic evidence:

(A) All records relating to violations of 21 U.S.C. 841(a) (drug trafficking) and/or 21 U.S.C. 846 (conspiracy to traffic drugs) involving [the suspect] since January 1, 2006, including lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's] schedule or travel from 1995 to the present; all bank records, checks, credit card bills, account information, and other financial records.

The terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks, ZIP disks, USB drives, memory sticks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

(B) Any copy of the X Company's confidential May 17, 2005 report, in electronic or other form, including any recognizable portion or summary of the contents of that report.

(C) ***[For a warrant to obtain records stored with an ISP pursuant to 18 U.S.C. Section 2703(a)]*** All stored electronic mail of any kind sent to, from and through the e-mail address [JDoe@isp.com], or associated with the user name "John Doe," account holder [suspect], or IP Address [xxx.xxx.xxx.xxx] / Domain name [x.com] between Date A at Time B and Date X at Time Y. Content and connection log files of all activity from January 1, 2006, through March 31, 2006, by the user associated with the e-mail address [JDoe@isp.com], user name "John Doe," or IP Address [xxx.xxx.xxx.xxx] / Domain name [x.x.com] between Date A at Time B and Date X at Time Y. including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable / DSL, T1 / LAN), ports used, telephone dial-up caller identification records, MAC address, and any other connection information or traffic data. All business records, in any form kept, in the possession of [Internet Service Provider], that pertain to the subscriber(s) and account(s) associated with the e-mail address [JDoe@isp.com], user name "John Doe," or IP Address [xxx.xxx.xxx.xxx] / Domain name [x.x.com] between Date A at Time B and Date X at Time Y, including records showing the subscriber's full name, all screen names associated with that subscriber and account, all account names associated with that subscriber, methods of payment, phone numbers, all residential, business, mailing, and e-mail addresses, detailed billing records, types and lengths of service, and any other identifying information.

Here are examples of how to describe the property to be seized when the computer hardware itself is evidence, contraband, or an instrumentality of a crime:

(A) Any computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, CDs, USB drives and floppy disks) that were or may have been used as a means to provide images of child pornography over the Internet in violation of 18 U.S.C. 2252A that were accessible via the Internet address www.[xxxxxxxx].com.

(B) Dell Inspiron Model 700m laptop computer with a black case.

II. DRAFTING AFFIDAVITS IN SUPPORT OF WARRANTS TO SEARCH AND SEIZE COMPUTERS

An affidavit to justify the search and seizure of computer hardware and/or files should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer played in the offense; and (3) an explanation of any special computer forensic issues, such as the need to remove the hardware or media for off-site imaging or forensic analysis. In addition, warrants that raise special issues (such as sneak-and-peek warrants, or warrants that may implicate the Privacy Protection Act, 42 U.S.C. 2000aa) require thorough discussion of those issues in the affidavit. Agents and prosecutors with questions about how to tailor an affidavit and warrant for a computer-related search may contact either their local CHIP or the Computer Crime & Intellectual Property Section at (202) 514-1026.

A. Background Technical Information

It may be helpful to include a section near the beginning of the affidavit explaining any technical terms that the affiant may use. Although many judges are computer literate, judges generally appreciate a clear, jargon-free explanation of technical terms that may help them understand the merits of the warrant application. At the same time, agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Here are some sample definitions:

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 Locator (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.

Cookies

A cookie is a file that is generated by a web site when a user on a remote computer accesses it. The cookie is sent to the user's computer and is placed in a directory on that computer, usually labeled "Internet" or "Temporary Internet Files." The cookie includes information such as user preferences, connection information such as time and date of use, records of user activity including files accessed or services used, or account information. The cookie is then accessed by the web-site on subsequent visits by the user, in order to better serve the user's needs.

Data Compression

A process of reducing the number of bits required to represent some information, usually to reduce the time or cost of storing or transmitting it. Some methods can be reversed to reconstruct the original data exactly; these are used for faxes, programs and most computer data. Other methods do not exactly reproduce the original data, but this may be acceptable (for example, for a video conference).

Denial of Service Attack (DoS Attack)

A hacker attempting a DoS Attack will often use multiple IP or email addresses to send a particular server or web site hundreds or thousands of messages in a short period of time. The server or web-site will devote system resources to each transmission. Due to the limited resources of servers and web-sites, this bombardment will eventually slow the system down or crash it altogether.

Domain

A domain is 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

A 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.com). A domain name can provide information about the organization, ISP, and physical location of a particular network user.

Encryption

Encryption refers to the practice of mathematically scrambling computer data as a communications security measure. The encrypted information is called "ciphertext." "Decryption" is the process of converting the ciphertext back into the original, readable information (known as "plaintext"). The word, number or other value used to encrypt/decrypt a message is called the "key."

File Transfer Protocol (FTP)

FTP is a method of communication used to send and receive files such as word-processing documents, spreadsheets, pictures, songs, and video files. FTP sites are online "warehouses" of computer files that are available for copying by users on the Internet. Although many sites require users to supply credentials (such as a password or user name) to gain access, the IP Address of the FTP site is often all that is required to access the site, and users are often identified only by their IP addresses.

Firewall

A firewall is a dedicated computer system or piece of software that monitors the connection between one computer or network and another. The firewall is the gatekeeper that certifies communications, blocks unauthorized or suspect transmissions, and filters content coming into a network. Hackers can sidestep the protections offered by firewalls by acquiring system passwords, "hiding" within authorized IP addresses using specialized software and routines, or placing viruses in seemingly innocuous files such as e-mail attachments.

Hacking

Hacking is the deliberate infiltration or sabotaging of a computer or network of computers. Hackers use loopholes in computer security to gain control of a system, steal passwords and sensitive data, and/or incapacitate a computer or group of computers. Hacking is usually done remotely, by sending harmful commands and programs through the Internet to a target system. When they arrive, these commands and programs instruct the target system to operate outside of the parameters specified by the administrator of the system. This often causes general system instability or the loss of data.

Hash Value

A hash value (or simply "hash"), also called a message digest, is a number generated from a *string of text or other data. The hash is substantially smaller than the data itself, and is generated by a mathematical algorithm formula in such a way that it is unique for that data set. If the original data is altered, the hash value will change. Similarly, if the hash values for two data sets match, it is reasonably certain that the two sets are identical.*

Hashes play a role in computer forensics where they are used to ensure that images of electronic media are accurately made by forensic software. They are also used in child pornography investigations to compare suspected child pornography images against known child pornography images.

Instant Messaging (IM)

IM is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are in the same state.

Internet

The Internet is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), 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 Relay Chat (IRC)

IRC is a popular Internet service that allows users to communicate with each other in real-time. IRC is organized around the "chat-room" or "channel," in which users congregate to communicate with each other about a specific topic. A "chat-room" typically connects users from different states and countries, and IRC messages often travel across state and national borders before reaching other users. Within a "chat-room" or "channel," every user can see the messages typed by other users.

No user identification is required for IRC, allowing users to log in and participate in IRC communication with virtual anonymity, concealing their identities by using fictitious "screen names." Furthermore, participants to IRC communications may enable logging, which will create a transcript of the chat- room communication.

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 such as cable TV, DSL or fiber optic service; 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. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data format and in written record format. ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a "remote computing service."

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 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 Internet service providers control a range of IP addresses.

Dynamic IP address

When an ISP or other provider uses dynamic IP addresses, the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a user dials into the ISP to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's IP address normally differs each time he dials into the ISP.

Static IP address A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.

Joint Photographic Experts Group (JPEG)

JPEG is the name of a standard for compressing digitized images that can be stored on computers. JPEG is often used to compress photographic images, including pornography. Such files are often identified by the ".jpg" extension (such that a JPEG file might have the title "picture.jpg") but can easily be renamed without the ".jpg" extension.

Log file

Log files are computer files that contain records about system events and status, the identity and 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. Logs can also maintain records regarding the identification of users on a network, as well as Internet sites accessed by the computer.

Moving Pictures Expert Group -3 (MP3)

MP3 is the name of a standard for compressing audio recordings (e.g., songs, albums, concert recordings) so that they can be stored on a computer, transmitted through the Internet to other computers, or listened to using a computer. Despite its small size, an MP3 delivers near CD-quality sound. Such files are often identified by the filename extension ".mp3," but can easily be renamed without the ".mp3" extension.

Packet Sniffing

On the Internet, information is usually transmitted through many different locations before it reaches its final destination. While in transit, such information is contained within "packets." Both authorized users, such as system security experts, and unauthorized users, such as hackers, use specialized technology - packet sniffers - to "listen" to the flow of information on a network for interesting packets, such as those containing logins or passwords, sensitive or classified data, or harmful communications such as viruses. After locating such data, the packet sniffer can read, copy, redirect, or block the communication.

Peer-to-Peer (P2P) Networks

P2P networks differ from conventional networks in that each computer within the network functions as both a client (using the resources and services of other computers) and a server (providing files and services for use by "peer" computers). There is often no centralized server in such a network. Instead, a search program or database tells users where other computers are located and what files and services they have to offer. Often, P2P networks are used to share and disseminate music, movies, and computer software.

Router

A router is a device on the Internet that facilitates communication. Each Internet router maintains a table that states the next step a communication must take on its path to its proper destination. When a router receives a transmission, it checks the transmission's destination IP address with addresses in its table, and directs the communication to another router or the destination computer. The log file and memory of a router often contain important information that can help reveal the source and network path of communications. Wireless computer networks utilize wireless routers that maintain information on computers that are connected to the wireless network.

Server

A server is 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 company, 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. Servers can serve as a location to store shared files, and can be used to store backup information regarding network activity.

In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

Steganography

The art and science of hiding information by embedding messages within other, seemingly harmless messages or graphic images. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different information that will not be visible to someone who views the files in the normal manner. This hidden information could be plain text, encrypted text, images, or any other sort of electronic data.

Tracing

Trace programs are used to determine the path that a communication takes to arrive at its destination. A trace program requires the user to specify a source and destination IP address. The program then launches a message from the source address, and at each "hop" on the network (signifying a device such as a router), the IP address of that device is displayed on the source user's screen or copied to a log file.

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.

Virus

A virus is a malicious computer program designed by a hacker to (1) incapacitate a target computer system, (2) cause a target system to slow down or become unstable, (3) gain unauthorized access to system files, passwords, and other sensitive data such as financial information, and/or (4) gain control of the target system to use its resources in furtherance of the hacker's agenda.

Once inside the target system, a virus may begin making copies of itself, depleting system memory and causing the system to shut down, or it may begin issuing system commands or altering crucial data within the system.

Other malicious programs used by hackers are, but are not limited to: "worms" that spawn copies that travel over a network to other systems, "trojan horses" that are hidden in seemingly innocuous files such as email attachments and are activated by unassuming authorized users, and "bombs" which are programs designed to bombard a target email server or individual user with messages, overloading the target or otherwise preventing the reception of legitimate communications.

B. Background - Staleness Issue

It may be helpful and necessary to include a paragraph explaining how certain computer files can reside indefinitely in free or slack space and thus be subject to recovery with specific forensic tools:

Based on your affiant's knowledge, training, and experience, including the experience of other agents with whom the affiant has spoken, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home 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.

C. Describe the Role of the Computer in the Offense

The next step is to describe the role of the computer in the offense, to the extent it is known. For example, is the computer hardware itself evidence of a crime or contraband? Is the computer hardware merely a storage device that may or may not contain electronic files that constitute evidence of a crime? To introduce this topic, it may be helpful to explain at the outset why the role of the computer is important for defining the scope of your warrant request.

Your affiant knows 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. 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 [images of child pornography, including those that may be stored on a computer]. These [images] constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware that may contain [the images of child pornography] if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Your affiant believes 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.

1. When the Computer Hardware Is Itself Contraband, Evidence, and/or an Instrumentality or Fruit of Crime

If applicable, the affidavit should explain why probable cause exists to believe that the tangible computer items are themselves contraband, evidence, instrumentalities, or fruits of the crime, independent of the information they may hold.

Computer Used to Obtain Unauthorized Access to a Computer ("Hacking")

Your affiant knows that when an individual uses a computer to obtain unauthorized access to a victim computer 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 computer hackers generally maintain records and evidence relating to their crimes on their computers. Those records and evidence may include files that recorded the unauthorized access, stolen passwords and other information downloaded from the victim computer, the individual's notes as to how the access was achieved, records of Internet chat discussions about the crime, and other records that indicate the scope of the individual's unauthorized access.

Computers Used to Produce Child Pornography

It is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can be connected toa video camera, VCR, or DVD-player, using a device called a video capture board: the device turns the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

2. When the Computer Is Merely a Storage Device for Contraband, Evidence, and/or an Instrumentality or Fruit of Crime

When the computer is merely a storage device for electronic evidence, the affidavit should explain this clearly. The affidavit should explain why there is probable cause to believe that evidence of a crime may be found in the location to be searched. This does not require the affidavit to establish probable cause that the evidence may be stored specifically within a computer. However, the affidavit should explain why the agents believe that the information may in fact be stored as an electronic file stored in a computer.

Child Pornography

Your affiant knows that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk can contain hundreds or thousands of images of child pornography, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection.

Illegal Business Operations

Based on actual inspection of [spreadsheets, financial records, invoices], your affiant is aware that computer equipment was used to generate, store, and print documents used in [suspect's] [tax evasion, money laundering, drug trafficking, etc.] scheme. There is reason to believe that the computer system currently located on [suspect's] premises is the same system used to produce and store the [spreadsheets, financial records, invoices], and that both the [spreadsheets, financial records, invoices] and other records relating to [suspect's] criminal enterprise will be stored on [suspect's computer].

D. Special Computer Forensics Issues

The affidavit should also contain a careful explanation of any special computer forensic issues that may impact upon the computer search.Such an explanation is particularly important when practical considerations require that agents seize computer hardware that is merely a storage device for evidence of crime and search it off-site. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail in order to provide adequate assurance to the reviewing court regarding the presence of these issues, and their consideration by the agents. Here is sample language that can apply in recurring situations:

1. Sample Language to Justify Seizing Hardware and Conducting a Subsequent Off-site Search

#. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. *Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.*

b. *Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures* *are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.*

c. *The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high. Further, a 160 GB drive could contain as many as approximately 150 full run movies or 150,000 songs.*

d. *Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.*

In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

2. Sample Language to Justify an Incremental Search

Generally, in the absence of a requirement by the magistrate, committing to an incremental search approach is not advised. However, some magistrates are requiring that applying agents demonstrate a willingness to minimize the impact of a computer seizure in a corporate environment. In such cases, the following language should be considered:

Your affiant recognizes that the [Suspect] Corporation is a functioning company with [approximately #]/ [numerous] employees, and that a seizure and removal of the [Suspect] Corporation's computer network may have the unintended and undesired effect of limiting the company's ability to provide service to its legitimate customers who are not engaged in [the criminal activity under investigation]. In response to these concerns, the agents who execute the search will take an incremental approach to minimize the inconvenience to [Suspect Corporation's] legitimate customers 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 all computers that are likely to store [the computer files described in the warrant]. 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. The computer forensic examiner or another technical expert will then conduct an off-site search for [the computer files described in the warrant] from the image copy at a later date.

B. *If "imaging" proves impractical, or even impossible for technical reasons, then the agents will seize those components of the [Suspect Corporation's] computer system that the computer forensic examiner believes must be seized to permit the agents to locate [the computer files described in the warrant] at an off-site location. The components will be seized and taken into the custody of the agent. If employees of [Suspect Corporation] so request, the computer forensic examiner will, to the extent practicable, attempt to provide the employees with copies of any files [not within the scope of the warrant] that may be necessary or important to the continuing function of the [Suspect Corporation's] legitimate business. If, after inspecting the computers, the analyst determines that some or all of this* *equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.*

3. Sample Language to Justify the Use of Comprehensive Data Analysis Techniques

Searching [the suspect's] computer system for the evidence described in [Attachment A] will require a range of computer forensic analysis techniques. 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. In order to properly execute the search authorized by the warrant, specially trained agents or forensic analysts will be required to conduct a thorough forensic analysis of the seized media, 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, your affiant requests permission to use whatever computer forensic analysis techniques appear necessary to locate and retrieve the evidence described in [Attachment A].

E. Special Considerations

The affidavit should also contain discussions of any special legal considerations that may factor into the search or how it will be conducted. These considerations are discussed at length in Chapter 2. Agents can use this checklist to determine whether a particular computer-related search raises such issues:

1. **Is the search likely to result in the seizure of any drafts of publications (such as books, newsletters, Web site postings, etc.) that are unrelated to the search and are stored on the target computer?** If so, the search may implicate the Privacy Protection Act, 42 U.S.C. 2000aa.

2. **Is the target of the search an ISP, or will the search result in the seizure of a mail server?** If so, the search may implicate the Electronic Communications Privacy Act, 18 U.S.C. 2701-12.

3. **Does the target store electronic files or e-mail on a server maintained in a remote location?** If so, the agents may need to obtain more than one warrant. Agents should be sensitive to the fact that these remote locations may be located in areas out of the jurisdiction of the issuing magistrate, and may be located outside of the United States.

4. **Will the search result in the seizure of privileged files, such as attorney-client communications? If so, special precautions may be in order, and special approval may be required. See the guidance in USAM 9-13.420.**

5. **Are the agents requesting authority to execute a "sneak-and-peek" search?** If so, the proposed search must satisfy the standard defined in 18 U.S.C. 3103a(b).

6. **Are the agents requesting authority to dispense with the "knock and announce" rule?**

[Return to Main Text]

APPENDIX G: Sample Letter for Provider Monitoring

[Note: as discussed in Chapter 4.D.3.c of this manual, agents and prosecutors should adopt a cautious approach to accepting the fruits of future monitoring conducted by providers under the provider exception. Furthermore, law enforcement may be able to avoid this issue by reliance on the computer trespasser exception. However, in cases in which law enforcement chooses to accept the fruits of future monitoring by providers, this letter may reduce the risk that any provider monitoring and disclosure will exceed the acceptable limits of 2511(2)(a)(i).]

This letter is intended to inform [law enforcement agency] of [Provider's] decision to conduct monitoring of unauthorized activity within its computer network pursuant to 18 U.S.C. 2511(2)(a)(i), and to disclose some or all of the fruits of this monitoring to law enforcement if [Provider] deems it will assist in protecting its rights or property. On or about [date], [Provider] became aware that it was the victim of unauthorized intrusions into its computer network. [Provider] understands that 18 U.S.C. 2511(2)(a)(i) authorizes

an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service[.]

This statutory authority permits [Provider] to engage in reasonable monitoring of unauthorized use of its network to protect its rights or property, and also to disclose intercepted communications to [law enforcement] to further the protection of [Provider]'s rights or property. Under 18 U.S.C. 2702(c)(3), [Provider] is also permitted to disclose customer records or other information related to such monitoring if such disclosure protects the [Provider]'s rights and property.

To protect its rights and property, [Provider] plans to [continue to] conduct reasonable monitoring of the unauthorized use in an effort to evaluate the scope of the unauthorized activity and attempt to discover the identity of the person or persons responsible. [Provider] may then wish to disclose some or all of the fruits of its interception, records, or other information related to such interception, to law enforcement to help support a criminal investigation concerning the unauthorized use and criminal prosecution for the unauthorized activity of the person(s) responsible.

[Provider] understands that it is under absolutely no obligation to conduct any monitoring whatsoever, or to disclose the fruits of any monitoring, records, or other information related to such monitoring, and that 18 U.S.C. 2511 (2)(a)(i) does not permit [law enforcement] to direct or request [Provider] to intercept, disclose, or use monitored communications, associated records, or other information for law enforcement purposes.

Accordingly, [law enforcement] will under no circumstances initiate, encourage, order, request, or solicit [Provider] to conduct nonconsensual monitoring absent an appropriate court order or a relevant exception to the Wiretap Act (e.g., 18 U.S.C. 2511(2)(i)), and [Provider] will not engage in monitoring solely or primarily to assist law enforcement absent such circumstances. Any monitoring and/or disclosure will be at [Provider's] initiative. [Provider] also recognizes that the interception of wire and electronic communications beyond the permissible scope of 18 U.S.C. 2511(2)(a)(i) may potentially subject it to civil and criminal penalties.

Sincerely,

General Counsel

[Return to Main Text]

APPENDIX H: Sample Authorization For Monitoring of Computer Trespasser Activity

This letter authorizes [law enforcement agency] to monitor computer trespasser activity on [Owner / Operator]'s computer. [Owner / Operator] maintains a computer [exclusively for the use of X financial institution(s) / the United States Government / that is used in interstate or foreign commerce / and the use of this computer by a financial institution or the United States Government is affected by such unauthorized activity]. Therefore, this computer is a "protected computer" under 18 U.S.C. 1030(e)(2).

An unauthorized user, without a contractual basis for any access, has accessed this computer, and is therefore a computer trespasser as defined by 18 U.S.C. 2510(21). The [Owner / Operator] understands that under 18 U.S.C. 2511 (2)(i)(I), [law enforcement agency] may not "intercept [the trespasser's] wire or electronic communications...transmitted to, through, or from" this computer without authorization from [Owner / Operator].

To protect its computer from the adverse effects of computer trespasser activity, the [Owner / Operator] authorizes [law enforcement agency] to monitor the communications of the trespasser to, through, and from this protected computer. The fruits of such monitoring may support a criminal investigation and possible prosecution of the person(s) responsible for such unauthorized use.

This authorization in no way represents consent to the interception, retrieval, or disclosure of communications other than those transmitted to or from the computer trespasser, and [law enforcement agency] may not acquire such communications in the course of its monitoring, pursuant to 18 U.S.C. 2511(3)(i)(IV), except under separate lawful authority.

Sincerely,

[Owner / Operator] General Counsel

[Return to Main Text]

ENDNOTES

1. "Electronic storage" is a term of art, specifically defined in 18 U.S.C. 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

2. 18 U.S.C. 2711(3) states "the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation."

3. "Electronic storage" is a term of art, specifically defined in 18 U.S.C. 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

4. An Internet Protocol (IP) address is a unique numerical address identifying each computer on the Internet. IP addresses are conventionally written in the dot-punctuated form *num1.num2.num3.num4* (*e.g.*, 192.168.3.47).

5. A "port" in the Transmission Control Protocol used over the Internet is a numeric identifier for a particular type of service being offered by a machine. For example, port 80 is typically reserved for World Wide Web traffic, so that a computer that wishes to retrieve information from a web server would typically connect to port 80. Often, however, hackers run programs which listen at a particular port, but do not provide the typically expected protocol at that port. These are often used as "back doors" into computer systems.

6. TCP port 25 is specifically reserved for the Simple Mail Transfer Protocol (commonly referred to as SMTP), port 80 is reserved for Hypertext Transfer Protocol (HTTP, or web traffic), port 110 is reserved for the Post Office Protocol version 3 (POP3), and port 143 is reserved for the Internet Mail Access Protocol (IMAP). **[Modify list of excluded ports as needed.]**