State of Missouri)
) ss.
County of Jackson)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, xxxx xxxxxxxxxx, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have served in this capacity since xxxxx x, xxxx. I am presently assigned to the St. Joseph, Missouri, Resident Agency, which is responsible for investigating violations of federal criminal law in the 17 northwest counties of Missouri. During this time, I have been assigned a wide variety of criminal investigations, including, but not limited to, child pornography, interstate transportation of sexually explicit material, and matters concerning the sexual exploitation of children. I have also had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media.

2. At all times throughout this affidavit I use the term "child pornography" merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction," "minor," and "sexually explicit conduct" as those terms are defined in Title 18, United States Code, Section 2256. (See Definition Section below).

3. The location to be searched is known as **xxxx xxxxxxxx xxxxxx, St. Joseph, Missouri, 64507** and this affidavit is submitted in support of a warrant to search the entire premises, including the residential premises, any outbuildings, and any computer and/or computer media found therein, where the instrumentalities, fruits, and/or evidence of violations of Title 18, United States Code, Section 2252, as further specified in **Attachment A**, might be located.

4. This affidavit is based upon information I have gained from my investigation, my training and experience, as well as information from other Special Agents of the Federal Bureau of Investigation and conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252 are located at the above address. Based upon the following information, there is probable cause to believe that currently located within the above-described premises is the evidence, fruits, and instrumentalities of trafficking, receipt, distribution, and/or possession of visual depictions, and other related materials, involving minors engaging in sexually explicit conduct (child pornography), as defined in Title 18, United States Code, Section 2256.

DEFINITIONS

5. The following definitions apply to this Affidavit and **Attachment A** to this

Affidavit:

a. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions;

b. "Child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct (See 18 U.S.C. § 2256(8)(A) only);

c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See 18 U.S.C. § 2256(5));

d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See 18 U.S.C. § 2256(2));

e. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device”;

f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks);

g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities;

h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items;

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which preform certain preset security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or

unusable, as well as reverse the progress to restore it;

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet; and

k. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Moreover, it has revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these pornographic images was accomplished through a combination of personal contact, mailings, and telephone calls. Naturally, any reimbursement would follow these same paths.

7. The development of computers has changed this. Computers serve four functions in connection with child pornography; these are, production, communication, distribution, and storage, which are illustrated as follows:

a. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device know as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and

technically easy to produce, store, and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as have been used in the past;

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device know as a modem allows any computer to connect to another computer through the use of telephone lines. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as CompuServe and America Online, which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web, hence they are commonly described as Internet Service Providers (ISPs). Some of these systems offer their subscribers the ability communicate publicly or privately with each other in real time in the form of "chat rooms";

c. Aside from "chat rooms" that reside on many service providers' networks, these ISPs allow access to a larger network of chat channels, one of which is called Internet Relay Chat (IRC), that is accessed through intermediary or "client software." Contact with other users in either of these “internal” or “external” online formats can be very open or anonymous - in front of everyone else who happens to be in the same room/channel at the same time, or very private and personal in the form of person to person instant messages;

d. Another type of this instant messaging that exists on the Internet is called ICQ. ICQ ("I Seek You") is a program which allows the user: to notify others of his online status (i.e., available, free for chat, away, etc.); to "page" another user by sending a message to the other user's computer; to transfer files, including text and graphic image files; to chat or communicate directly with one or more other users (up to an unlimited number); to save chat information in a text file for future access; and to communicate via E-Mail, among other things. A user's connection to ICQ and through ICQ to another user, is through a telephone line or a cable modem;

e. These communication structures are ideal for the child pornography collector. The open and anonymous communication allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other trusted child pornography collectors. Moreover, the child pornography collector need not use the large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors;

f. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail or through file transfer protocols[1] (FTP)) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide both electronic mail service, chat services and easy

access to the Internet, the computer is a preferred method of distribution of child pornographic materials;

g. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and to save the image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of the electronic storage devices is it possible to recreate the evidence trail;

h. Collectors and distributors of child pornography also use online resources

to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases; and

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

j. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Kazaa, one type of P2P software, sets up its searches by keyword. The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

k. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for either key words or previously identified child pornography files. The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the file(s) he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

l. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Kazaa user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a Kazaa user downloading an image file receives the entire image from one computer. On July 24, 2003, Phil Morle, Chief Technical Officer, Sharman Networks (developer of Kazaa P2P software) advised that if a Kazaa user receives only part of a file from a computer, the computer sending the partial file has the entire file.

m. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

n. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

8. Based on your affiant's knowledge, training, and experience, and the experience of other law enforcement personnel, your affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or laboratory. This is true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives, CDs, DVDs, PDAs, MMCs, memory sticks and optical disks) can store the equivalent of hundred of thousand of pagers of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification of destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

9. Based on your affiant's consultation with experts in computer searches, data retrieval from computers and related media and from his consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seized all of the computers system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices which allows users to enter or retrieve data from

the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the input/output devices, software, documentation, data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them in a reasonable period of time;

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). In cases like this one where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval; and

c. In addition, there is probable cause to believe the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of possession and transmitting child pornography in violation of federal law and should therefore all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

10. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a nonexclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. Surveying various file directories and the individual files they contain;

d. Opening files in order to determine their contents;

e. Scanning storage areas;

f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment A**; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment A**.

CONDUCT OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY

11. Pursuant to my training and experience, as well as the training and experience of other law enforcement personnel, your affiant has learned:

a. Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contact with other like-minded individuals who have it available;

b. The use of computers to traffic in, trade, or collect child pornography has become one of the preferred methods of obtaining child pornographic materials. An individual familiar with a computer can use it, usually in the privacy of his or her own home or office, to interact with another individual or business offering such material in this country or elsewhere in the world. The use of a computer provides individuals interested in child pornography with a sense of privacy and secrecy not attainable by other media. It also permits the individuals to contact and interact with many more individuals than through the use of the mails;

c. Persons involved in sending or receiving child pornography tend to retain it for long periods of time. This tendency is enhanced by the increased sense of security that a computer affords. In addition, your affiant is aware from training and guidance that persons who procure child pornography and who have a proclivity for sexual activity involving youths, obtain and retain magazines, films, videos, pictures, and other items of child pornography as well as correspondence, advertising, bills, and notes relating to sexual activity involving children for long periods of time and do not dispose of or destroy such materials excepts to trade such materials with others in exchange for similar items. In addition, such material is normally and generally kept in the individual's residence or other secure location to ensure convenient and ready access; and

d. Given the portability of computers, such as laptops, and the enormous capacity of CDs, DVDs, PDAs, MMCs, memory sticks and optical disks, evidence of child pornography is highly portable and can easily be transported within a vehicle.

12. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

a. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital, or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

b. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

c. The majority of individuals who collect child pornography maintain books, magazines, newspapers, and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

d. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

e. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. **THEY ALMOST ALWAYS MAINTAIN THEIR COLLECTIONS IN THE PRIVACY AND SECURITY OF THEIR HOMES OR OTHER SECURE LOCATION.**

THE INVESTIGATION

CONCLUSION

RESIDENCE DESCRIPTION

FURTHER AFFIANT SAYETH NOT.

xxxx xxxxxxxxxx, Special Agent
Federal Bureau of Investigation

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

xxxxxxx xxxxxxxx
CHIEF UNITED STATES MAGISTRATE JUDGE