**IN THE KANSAS DISTRICT COURT**

**ENTER JUDICIAL DISTRICT, ENTER YOUR COUNTY, KANSAS**

**CRIMINAL DIVISION**

**In Re: Application for Search Warrant: *Computer***

**STATE OF KANSAS**
**COUNTY OF:**

**v.**

**The Premises of:**

**Computer Brand, Model, Serial Number, Brief Description**

**Containing Electronic Media Storage (i.e. Hard Drive(s)):**

**Removable Media Seized**

**Currently located at:**

**Enter The Location And Description.**

**APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT PURSUANT TO K.S.A. 22-2502 AND SECTION 15 OF THE BILL OF RIGHTS OF THE KANSAS CONSTITUTION**

**STATE OF KANSAS**
**COUNTY OF SHAWNEE ss:**

I, ,
being first duly sworn upon my oath state:

**Section 1: Professional Identity and Experience:**

I am a duly certified law enforcement officer under the laws of the State of

Kansas employed by the:

I have approximately years of experience as a law enforcement officer and have had of hours of professional law enforcement training in the detection and investigation of criminal offenses. As a law enforcement officer, I

**Enter Relevant Experience Here.**

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.

In addition to my experience, I have attended numerous seminars and training classes, which include those taught by:

**ENTER Curriculum Vitae Or Brief Summary Classes.**

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.

## Section 2: Evidence of Crime:

The following evidence establishes probable cause to believe the following crime(s) have been or are being committed:

**Unlawful voluntary Sexual Relations 21-3522 a1**
**Sexual Exploitation of a child 21-3516 a1**
**Electronic Solicitation 21-3523a1**

**Enter The Case Facts**

## Section 3: Place to be searched:

This affidavit is made in support of and as an application for a search warrant to search the follow:

**Computer Brand, Model, Serial Number, Brief Description**

**Containing Electronic Media Storage (i.e. Hard Drive(s)):**

**Removable Media Seized**

**Section 4: To Be Seized:**

The evidence, fruits, and/or instrumentalities of crime to be seized are hereinafter described with particularity as:

**DEFINITIONS**

The following definitions apply to this Affidavit and Search Warrant:

"**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 ;

"**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;

"**Computer**," as used herein, is defined pursuant to, 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";

"**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);

"**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;

"**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;

"**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;

“**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

“**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).

**“Electronic Media Storage”** as used herein means any device designed to or capable of storing data or holding data in electronic format. (i.e. Hard Drive, Thumb Drives, Flash Memory, Floppy Disks, Compact Discs, DVDs,)

## BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

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.

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:

> 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 known 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;

Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market child pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect through the Internet to another computer through the use of telephone lines, cable lines, satellite, or wireless access points. By connecting to the Internet, electronic contact can be made to literally millions of computers around the world. Through Internet Service Providers (ISPs) providers users have access to electronic mail service between their own subscribers and those of other networks. 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" or "instant messaging" (IM); Many of these chat and IM programs also allow users to exchange, transfer, and / or simultaneously view image and movie files.

These communication structures are ideal for the child pornography collector. The open communication allows the user to locate others of similar inclination and still maintain relative 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. All of these advantages are well known and are the foundation of transactions between child pornography collectors;

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;

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 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.

Peer to peer file sharing (P2P) 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, LimeWire, FrostWire, and BearShare are popular examples of P2P software. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

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 (also known as "swarming download"). The advantage of this is that it speeds up the time it takes to download the file.

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.

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

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. The analysis of computer and/or digital media is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover digital information, to include hidden, erased, compressed, password-protected or encrypted files. The high volume of the contents and the potential intentional concealment of criminal activity through random ordering and deceptive file names may require the examination of all stored data. This process may take weeks or months depending on the volume of the data involved and the caseload of the computer expert. One such forensic and controlled laboratory environment is the Heart of America Regional Computer Forensics Laboratory (HARCFL), which is physically located in Clay County, Missouri. The HARCFL is a cooperative law enforcement organization comprised of federal, state and local certified Forensic Examiners that provide digital forensic services to law enforcement throughout Kansas and the western two-thirds of Missouri. The HARCFL is a nationally accredited laboratory certified by the American Society of Crime Laboratory Directors (ASCLD).

Recognizing that specialized and highly technical equipment and software will be needed to conduct the analysis of the previously seized digital media, the media will likely be transferred to the HARCFL or other qualified laboratory with a request that a forensic examination be conducted in this matter. Additionally, under limited situations, assistance may be required by the receiving laboratory from other qualified laboratories. I know that a specialized examiner is required because of the following:

1. 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;
2. 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.

3. The size of electronic storage media continues to grow, creating a large amount of data that must be searched to locate specific items. To place this in perspective, 250 GB hard drive can contain:
    a. up to 93,750 digital images;
    b. up to 221 days of around-the-clock MP3 ;
    c. up to 375 hours of VHS quality video or; 106 two-hour DVD-quality video.

Based on your affiant's consultation with experts in computer searches, data retrieval from computers and related media and from his consultations with other law enforcement officers 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:

> The peripheral devices which allow 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 (known as dongles). 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;

In order to fully retrieve data from a computer system, the analyst also needs all electronic storage devices. 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

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 law and should therefore all be seized as such.

Therefore I have reasonable belief that the seized media contains:

**Enter Items You Want To Recover**

**Section 5: Evidence of Probable Cause:**

The evidence of probable cause to believe that which is sought to be searched for and seized described with particularity and set forth above in Section 4 as evidence, fruits and/or instrumentalities of the crime and the evidence of probable cause to believe that such are now located in the premises to be searched as described in Section 3 above is set forth hereinafter:

**Facts and Probable Cause in Detail**

**WHEREFORE**, affiant respectfully requests that a Search Warrant issue authorizing the search of the premises described in Section 3 above and seizure of the property described in Section 4 above.

In witness whereof I have hereinforth subscribed my name and seal on this:

Date: Time: am pm

Subscribed and sworn to before me this:

Date: Time: am pm

District Court Judge

**IN THE KANSAS DISTRICT COURT**

**ENTER JUDICIAL DISTRICT, ENTER YOUR COUNTY, KANSAS**

**CRIMINAL DIVISION**

**In Re: Application for Search Warrant: *Computer***

**STATE OF KANSAS**
**COUNTY OF:**

**Enter Your County**

**v.**

**The Premises of:**

**Computer Brand, Model, Serial Number, Brief Description**

**Containing Electronic Media Storage (i.e. Hard Drive(s)):**

**Removable Media Seized**

**Currently located at:**

**Enter The Location And Description.**

## SEARCH WARRANT

**THE STATE OF KANSAS to Any and All Law Enforcement Officers of the State of Kansas:**

Having reviewed evidence before me under oath from which I have found probable cause to believe that a crime has been or is being committed, and sufficient facts have been presented to me under oath or affirmation which particularly describes the person, place or means of conveyance to be searched as identified in the caption hereof and such facts have established probable cause to believe that the following described articles have been used in the commission of a crime or are contraband or property which constitutes or may be considered a part of the evidence, fruits or instrumentalities of a crime, to-wit:

**Enter Items You Want To Recover**

And that there is probable cause to believe that the above-described articles to be seized are located in or on the above described premises or person to be searched.

**THEREFORE, YOU ARE COMMANDED** forthwith to search the person, place, thing, or means of conveyance described above within ninety-six (96) hours of the time and date of the issuance hereof and to seize the things described above to be seized and to hold them to be dealt with according to law.

This Search Warrant may be executed at any time of any day or night within ninety-six (96) hours of issuance within the:

**Enter Judicial District.**

On execution hereof you should make due return of this warrant and a copy hereof shall be provided the person searched or the person in possession or control of the premises or thing or means of conveyance searched and if such person is not present a copy together with a completed return shall be left on or in the premises, thing, or means of conveyance searched.

**ISSUED THIS:**

Date: Time: am pm

Reviewed By the District Attorney Office:

By:

**Judge of District Court**

**ENTER Judicial District**

**ENTER YOUR County, Kansas**

**OFFICER'S RETURN**

I received this Search Warrant on the:

Date: Time: am pm

and executed the same by searching the above described person, place, thing or means of conveyance described in said Search Warrant and seized the following:

Which I now have in my custody, possession or control subject to the further order of the Court, and, further, executed said warrant by arresting the within named:

before the Court.

A copy hereof was provided to:
or was left on or in the premises, place, thing, or means of conveyance searched for there was present no person whom was in possession or control of the same.

Date: Time: am pm

EXECUTING OFFICER:

AGENCY:

By:

Name:

Badge #