IN THE CIRCUIT COURT OF THE EIGHTH JUDICIAL CIRCUIT

IN AND FOR COUNTY COUNTY, FLORIDA

STATE OF FLORIDA, AGENCY CR #: 00-00-000000

Plaintiff,

-vs-     

SUSPECT(S), **APPLICATION AND AFFIDAVIT**

Defendant. **FOR SEARCH WARRANT**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

**APPLICATION FOR SEARCH WARRANT**

**BEFORE ME**, the undersigned Judge, State of Florida, came this sworn application and affidavit by YOUR RANK YOUR NAME, a law enforcement officer employed by the YOUR AGENCY, who was first duly sworn, deposes and says that HE/SHE (YOU) believes and has good reason to believe the laws of the State of Florida have been violated and are now being violated, and there is now being kept on or in the below described premises, and/or the curtilage of the same, certain evidence, fruits, or instrumentalities of a crime to be found in or on the following premises located in COUNTY County, Florida:

DESCRIBE THE LOCATION OF THE STRUCTURE YOU WANT TO SEARCH AS SPECIFICALLY. INCLUDE A DESCRIPTION OF THE BUILDING, THE COLOR, THE CURTILAGE AND THE GENERAL APPEARANCE IN AS MUCH DETAIL AS YOU ARE ABLE. The premises to be searched are located at ADDRESS, CITY, COUNTY, Florida.

To reach ADDRESS/LOCATION, SPECIFIC DIRECTIONS ON HOW TO REACH THE LOCATION.

SAID PREMISES being located in the County of COUNTY, State of Florida, in the control of the WHO HAS CONTROL OVER THE BUILDING, and being the property of WHO OWNS THE BUILDING and having within said premises, the following items to be seized:

1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data.  Hardware includes (but is not limited to) any data-processing devices, personal computers (i.e personal computers, laptops, notebooks), mobile electronic devices (i.e. tablets, smartphones, e-readers, gaming devices), game consoles (i.e. PlayStation, Xbox, etc.), internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).
2. Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.
3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks, flash drives, SD cards, or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.
4. Cloud based media storage systems (i.e. Dropbox, iCloud, Google Drive, etc.) or any other off-site media storage system with electronic access.
5. Computer software and application software installation and operation media.
6. Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.
7. Manuals and other documents (whether digital or written) which describe operation of items or software seized.
8. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.
9. Correspondence or other documents (whether digital or printed) pertaining to the possession, receipt, origin or distribution of images involving the exploitation of children.
10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.
11. Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and “zip” drive diskettes.  In particular, data in the form of images, and/or log files recording the transmission of images as they relate to violations of Florida law.

ALL OF WHICH are being kept and/or used and/or obtained in and/or is evidence of a felony violation of the laws of the State of Florida, to-wit:

Florida Statute 000.00 - OFFENSE NAME

Florida Statute 000.00 - OFFENSE NAME

THE BASIS for Your Affiant's belief is:

Your Affiant, YOUR RANK YOUR NAME (hereinafter referred to as YA), is a duly sworn law enforcement officer employed by the AGENCY and has been since HIRE DATE. YA successfully completed Basic Law Enforcement Training at ACADEMY YOU ATTENDED in CITY WHERE YOU ATTENDED, COUNTY WHERE YOU ATTENDED County, Florida. YA served as SUMMARIZE YOUR LEO WORK EXPERIENCE. YA has attended SUMMARIZE SPECIAL TRAINING & LEO CLASSES INCLUDING APPROXIMATE DATES OF COMPLETION. By HIS/HER training and experience, SUMMARIZE SPECIAL QUALIFICIATIONS BASED ON ABOVE TRAINING – IE, FAMILIARITY WITH CONTROLLED SUBSTANCES, KNOWLEDGE OF CHILD PORNGRAPHY, ETC. YA is currently assigned to CURRENT ASSIGNMENT, and has been assigned to investigate various criminal offenses to include, but not limited to, YOUR CASE LOAD since MONTH, YEAR YOUR CURRENT ASSIGNMENT BEGAN.

Based upon YA’S specialized:specialized training, education and experience, YA knows the following about the general operation and use of peer to peer (P2P) file sharing networks and programs:

1. A growing phenomenon on the Internet is peer to peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software.
2. 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.
3. 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 currently being shared on the network. A majority of the publicly available P2P software clients set up its searches by keywords. The results of a keyword search are displayed to the user. The user then selects file(s) from the results for download.
4. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the file. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." 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 sharing the file. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.
5. The strength of the P2P network is that it bases all of its file shares on a HASH value, specifically in this case the Secure Hash Algorithm (SHA1). SHA1 is a mathematical algorithm which allows for the comparison of files to ensure the files are the exact same, much the same as human fingerprints are compared and matched. Once a file is identified with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), the SHA1 value will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm standard for the Internet. The SHA1 is called secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.
6. 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.
7. The computer running the file sharing application has an IP address assigned to it while it utilizing the Internet. Investigators are able to observe the IP address of computer systems sharing files. Investigators can then search public records that are available on the Internet to determine the Internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can often be obtained from the Internet service provider.

The following information is known regarding the specific P2P file sharing network involved in this investigation:

1. The network is an open source public file-sharing network. Most computers that are part of this network are referred to as nodes. A node can simultaneously provide files to some peers while downloading files from other nodes. Nodes may be elevated to temporary indexing servers referred to as “supernodes.” Supernodes increase the efficiency of the network by maintaining an index of the contents of network peers. Users query supernodes for files and are directed to one or more peers sharing that file. There are many supernodes on the network, if one shuts down the network continues to operate.
2. The network can be accessed by computers running many different client programs, some of which include the original program, and derivatives compiled from the source code which is open source and freely available. These programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client.
3. During the installation of a client program, various settings are established which configure the host computer to share files. Depending upon the client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other users to download. This location is commonly referred to as the “My Shared Folder,” and in many versions is defaulted to be on the computer’s “Desktop.”
4. The client software processes files located in a user’s shared directory. As part of this processing, a SHA-1 hash value is computed for each file in the user’s shared directory.
5. The network uses SHA-1 values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA-1 values to ensure exact copies of the same file are used during this process.
6. Upon connecting to the network, a list of shared files, descriptive information and the files associated SHA-1 values are sent to supernodes. This allows other users to locate these files. The frequency of updating information is dependent upon the client software being used and the networking protocols. This information sent to the supernode is data about the file and not the actual file. The file remains on the user’s computer. In this capacity, the supernode acts as a pointer to the files located on a user’s computer.
7. When a download of a file is initiated, the user is presented with a list of users (nodes) who had told the network that they have the requested file available for others to download. Typically, the supernodes and host computers on the network return this list containing node information and the Internet Protocol (IP) addresses of computers which have reported they have the same file (based on SHA-1 comparison) or in some instances portions of the same file available to others to download. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography and files of interest (FOI) related to child pornography investigations.
8. Obtaining files from the network, as described herein, returns the candidate list, including IP addresses, which can be used to identify the location of computers. Although the IP address is not usually visible to the end user in the common clients, it is returned and used by the software to initiate the download.
9. Law Enforcement has modified the client program to allow the downloading of a file from a single IP address as well as displaying the IP address, which is known to all clients but not displayed.

SUMMARIZE YOUR CASE HERE

YA knows from training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files. YA also has knowledge that computer software or hardware exists that allows persons to share Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.  Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

YA knows that when a file is placed on a computer and subsequently relocated or deleted, electronic evidence remains on the computer to verify that the file existed on the system, or to recover the file as it existed at a certain point in time utilizing back-up or "shadow" copies. This electronic evidence can remain on the system for long periods of time, depending on various factors, such as the number of storage locations where the file was located, the length of time the image remained on the system, and the amount of data being stored or processed by the computer. In some circumstances, it is not unusual for electronic evidence confirming the existence of a file to remain on the computer for the life of the system.

YA knows from training and experience that computers used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of Internet service accounts used for the Internet access. Your Affiant is aware that search warrants of residences involved in computer related criminal activity usually produces items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

YA knows from training and experience that those who have demonstrated an interest in collecting sexually explicit visual images depicting adults and children (child pornography) are likely to keep these images concealed, but accessible.  The reasons offenders keep these images vary from offender to offender and collections are often maintained for multiple reasons.

YA knows from training and experience that child pornographic images may be kept as “trophies” such as actual photographs or images of the suspect’s own sexual activity with children.

YA knows from training and experience that an offender may also keep these images as a means of seducing the child victim by arousing curiosity, attempting to normalize the desired acts, lowering the inhibitions of potential child sexual partners by showing them that other adults and/or children participate in this kind of sexual activity and demonstrating and explaining what the offender may desire be done.  This process is generally referred to as “grooming.”

YA knows from training and experience that these images are also maintained as a means of sexually arousing the suspect.  In other instances, these images are maintained for commercial purposes, used to obtain money or other items of value including more child pornography.

YA knows from training and experience that child pornographic images tend to be extremely important to these offenders.  These images are likely to remain in the possession of or under their control for many years.  Because of their importance, it is unlikely an offender will destroy the images they have collected.  Likewise, if the individual has obtained child pornography via the Internet they rarely delete the material from their computer before printing or copying to other media.

Based on training and experience, YA is aware that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) and software to be searched later in a laboratory or other controlled environment. This is true because of the following:

1. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it 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 and invasive to attempt this kind of data search on site.
2. (2)Technical Requirements. 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 to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources and/or from destructive code imbedded in the system as a “booby trap”), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer 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.

In light of these concerns, YA hereby requests the Court’s permission to seize the above described items 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 and software for the evidence described.

BASED ON THE FOREGOING, YA has reason to believe and does believe that the structure in question has contained in the past, and does contain now, certain instrumentalities and contraband which constitutes a violation of the laws of the State of Florida, to-wit: Chapter 827 of Florida Statutes or certain evidence which constitutes proof of a violation of the laws of the State of Florida, and based upon the foregoing, requests issuance of a search warrant for the above-described residence to allow seizure of the above-described items.

WHEREFORE, Your Affiant prays that a search warrant be issued according to law commanding YA, and/or the Sheriff of Alachua County, or any of his duly constituted Agents, with proper and necessary assistance, to search the above-described residence for the above-described items, and for the seizure and safekeeping thereof, and for **authorization to search all of the said items** seized for child pornography either in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, in order that the evidence may be procured to be used in the prosecution of such person or persons unlawfully possessing or using the same in violation of the laws of the State of Florida.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                                          YOUR RANK YOUR NAME, Affiant

SWORN TO AND SUBSCRIBED before me this \_\_ day of MONTH, 20\_\_.

    SWORN TO AND

  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                                                          Notary or Assistant State Attorney

The above Application for Search Warrant coming on to be heard and having examined the application made under oath and the above sworn affidavit set forth and other facts and thereupon being satisfied that there is probable cause to believe that the grounds set forth in said Application and the facts do exist and that the law is being violated, I so find, and a search warrant is hereby allowed and issued.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                                                         JUDGE

 S.A. review: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ATTORNEY NAME

Assistant State Attorney

IN THE CIRCUIT COURT OF THE EIGHTH JUDICIAL CIRCUIT

IN AND FOR COUNTY COUNTY, FLORIDA

STATE OF FLORIDA, AGENCY CR #: 00-00-000000

Plaintiff,

-vs- SEARCH WARRANT

SUSPECT(S),

Defendant.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

IN THE NAME AND BY THE AUTHORITY OF THE STATE OF FLORIDA,

TO:   ALL AND SINGULAR THE SHERIFF AND/OR DULY CONSTITUTED DEPUTY SHERIFFS OF COUNTY COUNTY, FLORIDA, AND/OR DETECTIVES AND/OR LAW ENFORCEMENT OFFICERS OF LIST ALL LOCAL LE AGENCIES THAT MAY ASSIST WITH SERVICE, THE FLORIDA DEPARTMENT OF LAW ENFORCEMENT, AND/OR SPECIAL AGENTS OF THE UNITED STATES DRUG ENFORCEMENT ADMINISTRATION, AND/OR SPECIAL AGENTS OF THE UNITED STATES BUREAU OF ALCOHOL, TOBACCO, FIREARMS, AND EXPLOSIVES, AND/OR ANY OF THEIR DULY CONSTITUTED AGENTS

WHEREAS, complaint on oath and in writing, supported by affidavit has been made to me, the undersigned Judge of COUNTY County, Florida, by YOUR RANK YOUR NAME, a law enforcement officer employed by the YOUR AGENCY, who was first duly Sworn, deposes and says that HE/SHE (BASED ON YOU) has reason to believe the laws of the State of Florida have been violated and are now being violated and there is now being kept in or on the below-described premises and/or the curtilage of the same certain evidence, fruits, or instrumentalities of that crime to be found in or on the following described premises located in COUNTY County, Florida:

EXACT SAME DESCRIPTION USED IN YOUR APPLICATION (PAGE 1)

EXACT SAME DIRECTIONS TO PHONE USED IN YOUR APPLICATION (PAGE 1).

SAID ELECTRONIC DEVICE being located in the County of COUNTY, State of Florida, in the control of the WHO HAS CONTROL OF STRUCTURE, and being the property of WHO OWNS STRUCTURE, and Affiant having stated probable cause to believe that the following described items are upon/within said premises, the following are to be seized:

1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data.  Hardware includes (but is not limited to) any data-processing devices, personal computers (i.e personal computers, laptops, notebooks), mobile electronic devices (i.e. tablets, smartphones, e-readers, gaming devices), game consoles (i.e. PlayStation, Xbox, etc.), internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).
2. Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.
3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks, flash drives, SD cards, or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.
4. Cloud based media storage systems (i.e. Dropbox, iCloud, Google Drive, etc.) or any other off-site media storage system with electronic access.
5. Computer software and application software installation and operation media.
6. Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.
7. Manuals and other documents (whether digital or written) which describe operation of items or software seized.
8. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.
9. Correspondence or other documents (whether digital or printed) pertaining to the possession, receipt, origin or distribution of images involving the exploitation of children.
10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.
11. Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and “zip” drive diskettes.  In particular, data in the form of images, and/or log files recording the transmission of images as they relate to violations of Florida law.

ALL OF WHICH are being kept and/or used and/or obtained in and/or is evidence of a felony violation of the laws of the State of Florida, to-wit:

Florida Statute 000.00 - OFFENSE NAME

Florida Statute 000.00 - OFFENSE NAME

NOW THEREFORE, you or either of you, YOUR RANK YOUR NAME and officers with the above agencies, with such lawful assistance as may be necessary, are hereby commanded, in the daytime or in the nighttime, or on Sunday, or as the exigencies of the occasion may demand, to enter the said premises and the curtilage thereof, and then and there to search diligently for said property described in this warrant, and if the same or any part thereof be found on said premises, you are hereby authorized to seize, search, and secure the same, **and to conduct a further search, on-site and/or off-site, of any item seized**, and to make return of your doings under this warrant to a court with jurisdiction within ten days from the date hereof, and you are likewise commanded in the event you seize or take property or materials mentioned in the warrant to safely keep the same until otherwise ordered by a court having jurisdiction thereof, and that you give proper receipt for said property and deliver a copy of this warrant to the person from whom taken or those in whose possession it is found or in the absence of any such person to leave said copy in the place where said property or material is found, and you are further directed to bring said property so found and any person arrested in connection therewith before the court having jurisdiction of this offense to be disposed of according to law. You, or either of you, with such lawful assistance as may be necessary, are also authorized and commanded to search those vehicles and structures which you may encounter on the premises or curtilage thereof pursuant to the execution of this warrant.

WITNESS, my hand and official seal this \_\_\_ day of MONTH, 20\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

JUDGE