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 device, certain evidence, fruits, or instrumentalities of a crime to be found in or on the following premises located in COUNTY County, Florida:

DESCRIBE THE ELECTRONIC DEVISE YOU WANT TO SEARCH AS SPECIFICALLY AS YOU CAN. INCLUDE MAKE, MODEL, SERIAL NUMBER, COLOR, ETC. \*\*\*Do NOT open or operate phone to get description, just what you can see. The ELECTRONIC DEVICE to be searched is located at ITS CURRENT LOCATION INCLUDING ADDRESS, CITY, COUNTY, Florida.

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

SAID ELECTRONIC DEVICE being located in the County of COUNTY, State of Florida, in the control of the WHO HAS CONTROL OVER THE DEVICE, and being the property of WHO OWNS DEVICE and having within said electronic device, the following INFORMATION/PHOTOGRAPHS/ETC 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.

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 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.

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 electronic device 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, 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 electronic device 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 electronic device 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 electronic device certain evidence, fruits, or instrumentalities of that crime to be found in or on the following described electronic device 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 DEVICE, and being the property of WHO OWNS DEVICE, and Affiant having stated probable cause to believe that the following described items are upon/within said electronic device, 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 electronic device, 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 electronic device, 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