

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Middle District of Florida

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
A residence located at 85019 Miner Road,
Yulee, Florida 32097, more particularly
described in Attachment A

Case No. 3:17-mj- 1259-MCE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

A residence located at 85019 Miner Road, Yulee, Florida 32097, more particularly described in Attachment A.

located in the Middle District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.


The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 2252 & 2252A	Receipt and possession of child pornography.

The application is based on these facts:

See attached Affidavit.

- Continued on the attached sheet.
- Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature
FBI Special Agent Jonathan S. MacDonald

Printed name and title

Sworn to before me and signed in my presence

Date: 7/17/17

City and state: Jacksonville, Florida

I CERTIFY THE FOREGOING TO BE A TRUE
AND CORRECT COPY OF THE ORIGINAL
CLERK OF COURT

Judge's signature
UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
BY: DEPUTY CLERK

Richardson, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Jonathan S. MacDonald, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since November 2008 when I began my training at Quantico Virginia. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes. A portion of my duties are dedicated to investigating cases involving crimes against children under the auspice of the FBI's "Innocent Images" National Initiative. In the performance of my duties, I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2252 and 2252A, as well as Florida state statutes which criminalize the possession, receipt and transmission of child pornography, that is, visual images depicting minors engaged in sexually explicit conduct. I have been involved in over 100 searches pertaining to the possession, collection, production, and/or transportation of child pornography through either the execution of search warrants or through the subject providing written consent to permit a search.

2. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of securing a search warrant, and 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 evidence of violations of Title 18, United States Code, Sections 2252 and 2252A, is present in the residence and items to be searched.

STATUTORY AUTHORITY

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know the following:

a. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

b. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

c. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to knowingly possess, or knowingly access with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter, which contains one or more visual depictions of minors engaged in sexually explicit conduct that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer.

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign

commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(3) prohibits a person from knowingly reproducing child pornography for distribution through the mails or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

- e. The internet is a facility of interstate commerce.

DEFINITIONS

- 4. The following definitions apply 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, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-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, arithmetic 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. The terms "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, paintings), 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), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

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. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" 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 and is associated with a physical

address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different 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.

COMPUTERS AND CHILD PORNOGRAPHY

5. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and significant skill to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

6. The development of computers has radically changed the way that child pornographers manufacture, obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

7. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, images and videos can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

8. A 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, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

9. The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, and Google, 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.

11. As is the case with most digital technology, communication 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 email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos 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). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were

traded over the Internet. 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 P2P software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

12. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, I know that searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (*e.g.*, hard drives, compact disks ("CDs"), diskettes, tapes, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of

data stored, and it would be generally impossible to accomplish 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 should analyze the system and its data. The search of a computer system, which includes the use of data search protocols, is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased,¹ compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

13. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals

¹ Based on my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that computer forensic techniques can often recover files, including images and videos of child pornography, that have long been "deleted" from computer media by a computer user.

who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography also collect other 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. Many of these individuals also collect child erotica, which may consist of images or text that do not meet the legal definition of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many 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 in children and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), 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 often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email 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.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually

explicit materials as prized and valuable materials, even as commodities to be traded with other like-minded individuals over the Internet. As such, they tend to maintain or “hoard” their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. These individuals may protect their illicit materials by passwords, encryption, and other security measures; save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted; or send it to third party image storage sites via the Internet. Based on my training and experience, as well as my conversations with other experienced law enforcement officers who conduct child exploitation investigations, I know that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often maintain and/or possess the items listed in Attachment B.

14. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials. For example, I am familiar with the facts of an investigation conducted in the Middle District of Florida. In this investigation, the subject had his residence searched pursuant to a federal search warrant and his computer and digital storage media seized by the FBI. The search of his computer and other computer storage media revealed the subject knowingly possessed several

thousand images of child pornography. The subject retained an attorney and both were made aware of the ongoing investigation into the subject's commission of federal child pornography offenses. Approximately two months later, the subject was arrested on federal child pornography possession charges. After the subject's arrest, the FBI obtained a laptop computer owned by the subject's employer but possessed and used by the subject both before and after the execution of the search warrant at his residence. Subsequent forensic examination of this computer revealed that the subject had downloaded, possessed and viewed images of child pornography numerous times *after* the execution of the search warrant and before his arrest. Based on my training and experience, as well as conversations with other experienced law enforcement officers and forensic computer examiners, I also know that with the development of faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some individuals have also been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. However, as referenced above, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favored images involving a particular child or act is often maintained on this device.

15. Based on my training and experience, I also know that, with the development of faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. However, as referenced above, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favored images involving a particular child or act is often maintained on the device.

**PEER-TO-PEER (P2P) FILE
SHARING AND SHA-1 VALUE FILE IDENTIFICATION**

16. Peer-to-peer file sharing ("P2P") is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers directly together instead of through a central server. Computers that are part of this network are referred to as "peers" or "clients." There are several different software applications that can be used to access these networks, but these applications operate in essentially the same manner. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the

Internet. This software is used exclusively for the purpose of sharing digital files over the internet.

17. The BitTorrent network is a very popular and publicly available P2P file sharing network. A peer/client computer can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network programs, examples of which include the BitTorrent client program, the μ Torrent client program, the Vuze client program, and the BitComet client program, among others.

18. During the installation of typical BitTorrent network client programs, various settings are established that configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, these other peers/clients on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. The reassembly of pieces of files is accomplished by the use of hash values, which are described more fully below. Once a user has completed the download of an entire file or files, the user can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files. A host computer that has all the pieces of a file available for uploading to the internet is termed a "seeder." Using the BitTorrent protocol, several basic computers, such as home computers, can replace large servers while efficiently distributing files to many recipients.

19. Files or sets of files are shared on the BitTorrent network through the use of "Torrents." A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but rather contain information about the file(s) to be shared. This information includes the "info hash," which is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent. The term SHA-1 is a shorthand term for the hash value calculated by the Secure Hash Algorithm. The Secure Hash Algorithm (SHA-1) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA-1 hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA-1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA-1 signature are identical copies of the same file regardless of their file names. The data contained in the Torrent information includes the SHA-1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This "info hash" uniquely identifies the Torrent file on the BitTorrent network.

20. In order to locate Torrent files of interest and download the files that they describe, a typical user will use keyword searches on Torrent-indexing websites,

examples of which include *isohhunt.com* and the *piratebay.org*. Torrent-indexing websites do not actually host the content (files) described in and by the Torrent files, only the Torrent files themselves or a link that contains that SHA-1 hash value of the Torrent or the files being shared. Once a Torrent file is located on the website that meets a user's keyword search criteria, the user will download the Torrent file to their computer. The BitTorrent network client program on the user's computer will then process that Torrent file to help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the Torrent file.

21. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a Torrent-indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). Based on the results of the keyword search, the user would then select a Torrent of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the Torrent file. Using BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the Torrent file and that these file(s) are available for sharing. The user can then download the file(s) directly from the computer(s) sharing them. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file(s) with other users on the network. The downloaded file(s) are then stored in an area or folder previously designated by the user's computer or on an external storage

media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user.

22. Law enforcement can search the BitTorrent network in order to locate individuals sharing child pornography images, which have been previously identified as such based on their SHA-1 values. Law enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

23. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes (1) the suspect client's IP address; (2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and (3) the BitTorrent network client program and version being used by the suspect computer. Law enforcement can then log this information.

24. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are

associated with the Internet Crimes against Children (ICAC) Task Force Program. The ICAC Task Force Program uses law enforcement tools to track IP addresses suspected (based on SHA1 values and file names) of trading child pornography. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of whom were also involved in contact sexual offenses against child victims.

25. Based on my training and experience, as well as conversations with other experienced law enforcement officers, I know that cooperating police agencies pool their information to assist in identifying criminal conduct and build probable cause to further criminal investigations. With this pooled information, law enforcement officers may obtain a better understanding of the global information available about a suspect that resides within their geographic area of jurisdiction. Given the global scope of the Internet, this information is valuable when trying to establish the location of a suspect. Investigators from around the world gather and log information, which can be used by an investigator to establish probable cause for a specific investigation in his or her jurisdiction.

**BACKGROUND OF INVESTIGATION AND
FACTS ESTABLISHING PROBABLE CAUSE**

26. I make this affidavit in support of a search warrant for the residence located at 85019 Miner Road, Yulee, Florida 32097 that I believe to be currently occupied by Charles Cory Thornton (date of birth 08/03/1980) and Charles Emory

Thornton (date of birth 10/07/1949). This affidavit is based on information provided to me both verbally and in written documentation from other law enforcement officers and personnel, including FBI Staff Operations Specialist (SOS) Karen Ryndak and Task Force Officer (TFO) Jimmy Watson, as well as through investigation that I personally conducted as set forth herein. I have personally observed the residence, and it appears as set forth in Attachment A.

27. The FBI is investigating Charles Cory Thornton and Charles Emory Thornton as potential suspects for using one or more computers and computer media at this residence to commit violations of Title 18, United States Code, Sections 2252 and 2252A, which prohibit mailing, transportation, shipment, receipt, distribution, possession and access with intent to view, in interstate or foreign commerce by any means, including by computer, any child pornography, that is, visual depictions of one or more minors engaging in sexually explicit conduct.

28. FBI TFO Jimmy Watson has advised me of and provided the FBI with the following information, some of which was set forth in written documentation that I have reviewed. On January 24, 2016, TFO Watson began an undercover operation to identify persons using the BitTorrent P2P network on the Internet to receive, traffic in, share and/or distribute images and videos depicting child pornography. I know that TFO Watson has received training in the operation and use of the BitTorrent P2P network, as well as certain law enforcement techniques used to investigate users on this network. TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the

BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 98.231.62.250 had previously been associated with certain Files of Interest (FOI)² by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

29. Between January 24, 2016 and March 8, 2016, a law enforcement computer used and controlled by TFO Watson made 17 successful connections to a host computer at IP address 98.231.62.250 using an undercover computer through the Internet. As described herein, the following specific connections were made to a host computer at IP address 98.231.62.250 by a law enforcement computer controlled by TFO Watson. I know the above information based on conversations with TFO Watson and also from my review of his investigative reports which were submitted into the FBI's case file management system.

a. Between January 25 and 26, 2016, this law enforcement computer successfully downloaded 259 pieces of a total of 259 pieces of a video file

² Based on my training and experience, I know that the term "File(s) of Interest" refers to digital video and/or image files that depict child pornography and/or child erotica. These FOIs have previously been encountered, viewed, and catalogued by law enforcement personnel and/or staff working in and/or with ICAC task forces around the country. The descriptions and unique SHA-1 values of these FOIs are posted by ICAC investigators to the secure ICAC website for use by other ICAC trained online undercover investigators in confirming whether particular files in their respective investigations constitute child pornography or child erotica. As a law enforcement officer who specializes in the investigation of crimes against children, I have access to this secure ICAC website and have experience using it to identify and classify images and videos of suspected child pornography.

from the host computer at IP address 98.231.62.250, and through this connection it was confirmed that this host computer possessed all pieces.

b. On February 3, 2016, this law enforcement computer successfully downloaded 1 piece of a total of 4,551 pieces of an image and video collection from the host computer at IP address 98.231.62.250, and through this connection it was confirmed that this host computer possessed 4,394 pieces.

30. Subsequently, I reviewed the image and video portions that TFO Watson caused to be downloaded from the host computer connected to the Internet through IP address 98.231.62.250 between January 24, 2016 and March 8, 2016. Based on my training and experience, I believe that the image and video files depict at least one minor engaged in sexually explicit conduct, and therefore constitute child pornography pursuant to Title 18, United States Code, Section 2256. As described herein, the SHA-1 values for the files are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). Two of the files that TFO Watson caused to be downloaded from IP address 98.231.62.250 during the connections between January 25 and 26, 2016 and on February 3, 2016 that were being offered for sharing, are described as follows:

SHA-1: 2558f2908b932880893e1b2e01cde28fd3708c7b

DATE: Between January 25, 2016 at 6:42 p.m. Eastern Standard Time
(EST) and January 26, 2016 at 12:26 a.m. EST

TITLE: Slut Girlchild 10Yo movie_(244).avi

DESCRIPTION: This is a color video of 2:22 (minutes: seconds) duration, of which the entire video was downloaded directly from a host computer at IP address 98.231.62.250. I have reviewed this video. This is a color video file which begins with a prepubescent female child performing oral sex on an adult male's erect penis. The female child is wearing a button up shirt which is unbuttoned, displaying her chest and a lack of any breast development. At approximately 0:43, the camera changes to a close-up of the female child's face and open mouth. The female child then removes her shirt and opens her mouth at the tip of the adult male's erect penis as he masturbates. The adult male then ejaculates into the female child's mouth and she turns to the side, spitting the ejaculate onto the ground. The adult male then rubs his penis repeatedly across the female child's mouth. The video concludes with a close up view of the child's mouth.

SHA-1: 7be28dcb273417bf1877dca9a5e981c561adc524

DATE: February 3, 2016 between 1:17 a.m. and 9:48 a.m. EST

TITLE: Pictures from ranchi torpedo dloaded in 2009-pedo kdv kidzilla
pthc toddlers 0yo 1yo2yo 3yo 4yo 5yo 6yo 9yo tara babyj (179)

DESCRIPTION: This is a color image downloaded directly from a host computer at IP address 98.231.62.250. I have reviewed this image. This image depicts a female toddler-aged child lying on her back with her legs spread. An adult male is seen in front of the female child with his erect penis in his left hand, penetrating the female vaginally. There appears to be ejaculate (semen) pooled on the female's genitalia.

31. Through the use of Arin, a publicly available online resource, the IP address 98.231.62.250 was determined to be issued to Comcast Communications.

32. On June 16, 2016, FBI Operational Support Technician (OST) James Guy prepared an administrative subpoena directed to Comcast Communications requesting the subscriber name associated with IP address 98.231.62.250 for the period between January 24, 2016 and February 3, 2016.

33. Also on June 16, 2016, the Comcast Legal Response Center responded to this subpoena and provided the following information that I have reviewed. The subscriber information for the IP address 98.231.62.250 during the periods between January 24, 2016 and February 3, 2016 resolved back to the account of Charles Thornton, 85019 Miner Road, Yulee, Florida 32097. The email address associated with this account is cthorn4540@comcast.net.

34. FBI SOS Karen Ryndak has advised me of and provided me with the following information, some of which was set forth in written documentation that I have reviewed. On September 13, 2016, SOS Ryndak began an undercover operation to identify persons using the BitTorrent P2P network on the Internet to receive, traffic in, share, and/or distribute images and videos depicting child pornography. I know that SOS Ryndak has received training in the operation and use of the BitTorrent P2P network, as well as certain law enforcement techniques used to investigate users on this network. SOS Ryndak was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, SOS

Ryndak was able to determine that a host computer using IP address 50.159.189.79 had previously been associated with certain FOI by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

35. Between September 13, 2016 and September 15, 2016, a law enforcement computer used and controlled by SOS Karen Ryndak made three successful connections to a host computer at IP address 50.159.189.79 using an undercover computer through the Internet. On September 15, 2016, a law enforcement computer used and controlled by SOS Ryndak made a successful connection to a host computer at IP address 50.159.189.79 using an undercover computer through the Internet. Using this connection and specialized software, this law enforcement computer successfully downloaded 171 pieces of a total of 482 pieces of multiple photo files from the host computer at IP address 50.159.189.79 and through this connection it was confirmed that this host computer possessed 171 pieces. I know the above information based on conversations with SOS Ryndak and also from my review of her investigative reports which were submitted into the FBI's case file management system.

36. Subsequently, I reviewed portions of the image files that SOS Ryndak caused to be downloaded from the host computer connected to the Internet through IP address 50.159.189.79 on September 15, 2016. Based on my training and experience, I believe that the images depict at least one minor engaged in sexually explicit conduct, and therefore constitute child pornography pursuant to Title 18,

United States Code, Section 2256. As described herein, the SHA-1 values for each of these images are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the ICAC. An image file that SOS Ryndak caused to be downloaded from IP address 50.159.189.79 during September 15, 2016 that was being offered for sharing at the times listed below is described as follows:

SHA-1: ce39751e569a90030945551fec582bcc44f278a8

DATE: September 15, 2016 between 2:01 p.m. and 2:50 p.m. EDT

TITLE: 14.jpg

DESCRIPTION: This is a color image downloaded directly from a host computer at IP address 50.159.189.79. I have reviewed this image. This image depicts what appears to be a prepubescent female minor from the mid-stomach to mid-thighs with her legs spread lying on a blue sheet, with what also appears to be a white and yellow striped fabric between her legs. The focal point of the image is the minor's genitalia. The minor child does not have any visible pubic hair.

SHA-1: 4123e840ba491b9c28e9e8171a89c5aea153fbab

DATE: September 15, 2016 between 2:01 p.m. and 2:50 p.m. EDT

TITLE: liltoy.jpg

DESCRIPTION: This is a color image downloaded directly from a host computer at IP address 50.159.189.79. I have reviewed this image. This image depicts a nude prepubescent female child lying on her back with legs spread displaying her genitalia as the focal point of the image. The minor child is spreading

a yellow slinky toy across her chest. The minor child does not have any visible pubic hair and has child-sized arms and legs and child-like facial features.

37. Through the use of Arin, a publicly available online resource, the IP address 50.159.189.79 was determined to be issued to Comcast Communications.

38. At the request of SOS Ryndak, on September 21, 2016, FBI OST Kelsey Knecht prepared an administrative subpoena directed to Comcast Communications requesting subscriber information for IP address 50.159.189.79 for the period between September 13, 2016 at 3:01 a.m. and September 14, 2016 at 3:04 a.m. EDT.

39. On September 23, 2016, the Comcast Legal Response Center responded to this administrative subpoena and provided the following information that I have reviewed. The subscriber information for the IP address 50.159.189.79 during the periods between September 13, 2016 at 3:01 a.m. and September 14, 2016 at 3:04 a.m. EDT resolved back to the account of Charles Thornton, 85019 Miner Road, Yulee, Florida 32097. The email address associated with this account is cthorn4540a@comcast.net.

40. FBI TFO Jimmy Watson has advised me of and provided the FBI with the following information, some of which was set forth in written documentation that I have reviewed. On November 13, 2016, TFO Watson began an undercover operation to identify persons using the BitTorrent P2P network on the Internet to receive, traffic in, share and/or distribute images and videos depicting child pornography. I know that TFO Watson has received training in the operation and

use of the BitTorrent P2P network, as well as certain law enforcement techniques used to investigate users on this network. TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 66.177.109.249 had previously been associated with certain FOI by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

41. Between November 13, 2016 and March 2, 2017, a law enforcement computer used and controlled by FBI TFO Jimmy Watson made 186 successful connections to a host computer at IP address 66.177.109.249 using an undercover computer through the Internet. As described herein, the following specific connection was made to a host computer at IP address 66.177.109.249 by a law enforcement computer controlled by TFO Watson. I know the above information based on conversations with TFO Watson and also from my review of his investigative reports which were submitted into the FBI's case file management system.

a. Between January 5 and 6, 2017, this law enforcement computer successfully downloaded 377 pieces of a total of 532 pieces of multiple image and video files from the host computer at IP address 66.177.109.249, and through this connection it was confirmed that this host computer possessed 377 pieces.

42. Subsequently, I reviewed the portions of the video and image files that FBI TFO Watson caused to be downloaded from the host computer connected to the Internet through IP address 66.177.109.249 between January 5, 2017 and January 6, 2017. Based on my training and experience, I believe that the video and image files depict at least one minor engaged in sexually explicit conduct, and therefore constitute child pornography pursuant to Title 18, United States Code, Section 2256. As described herein, the SHA-1 values for each of these video portions are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). And image and video that FBI TFO Watson caused to be downloaded from IP address 66.177.109.249 during the period between January 5 and January 6, 2017 that were being offered for sharing on the dates and times listed below, are described as follows:

SHA-1: c17b1679e71c84f4a32e68fb4538ee4a84e0fe6b

DATE: Between January 5, 2017 at 10:36 p.m. and January 5, 2017 at 9:39 p.m. EST

TITLE: pthc 9yo Jenny daughter tied up and dog licking her.avi

DESCRIPTION: This is a color video file approximately 2:06 (minutes: seconds) in length, of which the entirety was downloaded directly from a host computer at IP address 66.177.109.249. The video begins with a naked pre-pubescent female child lying on her back with her legs spread on a purple towel. The female child is blindfolded and bound at the wrists and ankles with a yellow colored

rope. A brown colored dog is seen licking the vagina of the prepubescent female child. At approximately 0:13, the dog stops licking the female child's vagina and the camera zooms into a close up view of the child's vagina as she is digitally penetrated. An adult male hand then enters the frame, touching the female child's vagina and motioning for the dog to resume licking. At approximately 0:38, the adult male adds a substance to the female child's vagina to encourage the dog to continue licking. As the dog continues to lick her vagina, the camera moves to show the female child performing oral sex on an adult male penis. The video concludes with the adult male rubbing and opening the female's vagina so as to encourage the dog to continue licking. The prepubescent female child is a known victim previously identified by law enforcement and NCMEC as being nine years of age at the time of the production of this video.

SHA-1: c2629e63b1406bc9bc7109c447872c7a0a872945

DATE: Between January 5, 2017 at 10:36 p.m. and January 5, 2017 at 9:39 p.m. EST

TITLE: pthc_ptsc_9yo_jenny_enjoying_doggie_cock.jpg

DESCRIPTION: This is a color image file downloaded directly from a host computer at IP address 66.177.109.249. I have reviewed this image. This image depicts a prepubescent female child performing oral sex on an erect male dog's penis. The prepubescent female child is a known victim previously identified by law enforcement and NCMEC as being nine years of age at the time of the production of this image.

43. Through the use of Arin, a publicly available online resource, the IP address 66.177.81.249 was determined to be issued to Comcast Communications.

44. At the request of SA Joseph A. Barriere, on March 30, 2017, FBI OST Knecht prepared an administrative subpoena directed to Comcast Communications requesting any IP address associated with Charles Cory Thornton at 85019 Miner Road, Yulee, Florida 32097, for the period between October 1, 2016 and March 29, 2017.

45. On April 10, 2017, the Comcast Legal Response Center responded to this administrative subpoena and provided the following information that I have reviewed. The IP address designated to the account of Charles Thornton during the periods between October 13, 2016 and Mar 29, 2017 was IP address 66.177.81.249.

46. On May 3, 2017, SA Barriere conducted a query of the Florida Drivers and Vehicle Information Database (DAVID) for persons holding a State of Florida Driver's License or Identification Card residing at 85019 Miner Rd, Yulee, Florida 32097. This query revealed Florida driver's licenses issued to the following persons residing at this address: Charles Cory Thornton (date of birth 08/03/1980) and Charles Emory Thornton (date of birth 10/07/1949).

47. On June 22, 2017 at approximately 4:02 p.m. EDT, SOS Ryndak queried the ICAC secure website and queried the recent history of the user using the IP address 66.177.109.249. This revealed that this user was last observed utilizing this IP address on the BitTorrent P2P network on May 31, 2017.

48. On July 13, 2017, at my request, FBI OST Knecht prepared an administrative subpoena directed to Comcast Communications requesting any IP address associated with Charles Cory Thornton at 85019 Miner Road, Yulee, Florida 32097, for the period between May 31, 2017 to the present.

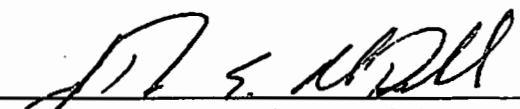
49. On July 14, 2017, the Comcast Legal Response Center responded to this administrative subpoena and provided the following information that I have reviewed. Comcast Communications provided results that confirmed active service to the account of Charles Thornton during the periods between May 31, 2017 and July 12, 2017 at the residence located at 85019 Miner Road, Yulee Florida 32097.

CONCLUSION

48. Based on the foregoing, I have probable cause to believe that one or more individuals has used and is using one or more computers and/or electronic storage media located in the residence located at 85019 Miner Road, Yulee, Florida 32097, more fully described in Attachment A to this affidavit, to, among other things, receive and possess child pornography. Therefore, I have probable cause to believe that one or more individuals, using the residence described above has violated 18 U.S.C. §§ 2252 and 2252A. Additionally, I have probable cause to believe that fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including at least one computer and other electronic storage media containing images of child pornography, and the items more fully described in Attachment B to this affidavit (which is incorporated by reference herein), will be located in this residence.

49. Through my training and experience, I know that individuals often travel with portable electronic devices, such as cell phones, smart phones, laptop computers, and other external storage or media devices, and that occasionally those devices may be temporarily stored or left, either intentionally or intentionally, in vehicles used by the device's user. Additionally, I know that the premises to be searched has a detached garage with two side-by-side overhead garage doors that is adjacent to the primary residence and appears capable of holding two vehicles, and is also capable of containing and concealing the items set forth in Attachment B. Therefore, this application specifically seek authority to search, in addition to the primary residence described in Attachment A, the detached garage set forth in Attachment A, and any vehicle located on the premises.

50. Accordingly, I respectfully request a search warrant be issued by this Court authorizing the search and seizure of the items listed in Attachment B.



Jonathan S. MacDonald, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this
17th day of July, 2017, at Jacksonville, Florida.



MONTE C. RICHARDSON
United States Magistrate Judge

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the residence, including the detached garage, any vehicles, and/or other independent structures capable of concealing the items listed in Attachment B herein, located on the premises at 85019 Miner Road, Yulee, Florida 32097. The primary residence is a single story, single family dwelling located near the junction of Miner Road and Haddock Road. The structure's exterior is comprised of a tan siding façade on top of a gray colored brick foundation. The front door is centered on the east wall facing Miner Road and appears to be painted dark brown. To the right of the front door (when facing the residence looking northward from Miner Road) are two windows, each with one glass pane, framed in dark brown. To the left of the front door (when facing the residence looking northward from Miner Road) are two windows, the first with two glass panes and the second with one glass pane, framed in dark brown. The residence has light brown colored shingles. A straight driveway leads from Miner Road to the north side of the residence and then turns south to the back of the residence ending at the back door stoop. Located in the back yard is a detached two-car garage facing east with a concrete parking pad to the east and extending eight feet to the south. The front yard features some grass and several large trees. A gray colored chain link fence appears to enclose the front yard and back yard. A gray-colored mailbox, located directly across Miner Road from the residence, has the numbers "85019" affixed to the right

side of the mailbox and the numbers "85019" written in black marker stencil on the right bottom side of the mailbox.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, "smart" phones such as an Apple iPhone, electronic tablets such as an Apple iPad, digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images), computer-related documentation, computer passwords and data-security devices, videotapes, video-recording devices, video-recording players, and video display monitors that are or may be used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs, including peer-to-peer software, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs

and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries or address books containing names or lists of names and addresses of individuals who have been contacted by use of the computer(s) or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and

electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an internet service provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other

remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment capable of being used to produce, manufacture, store and/or conceal visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises to be searched, including rental or lease agreements,

mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, logs, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the identity of any and all owners and/or users of any computers, computer media and any electronic storage devices discovered in the premises and capable of being used to produce, manufacture, store and/or conceal visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).