ATTACHMENT C
UNITED STATES DISTRICT COURT
DISTRICT OF MONTANA, MISSOULA DIVISION
AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

Your affiant, Richard McManaway, a Special Agent with the Homeland Security Investigation (HSI), Kalispell, Montana Resident Agency in Charge, being duly sworn, depose and state as follows, to wit:

Your affiant is submitting this Affidavit under Rule 41 of the Federal Rules of Criminal Procedure in support of an Application for a Search Warrant authorizing a search of the residential property at 1035 2nd Avenue West, Kalispell, Montana, and any person located at that property, more particularly described in Attachment A.

The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. § 2252A(a)(1), which makes it a crime to transport or ship in interstate or foreign commerce, by computer, child pornography, 18 U.S.C. § 2252A(a)(5), which makes it a crime to view and possess child pornography, and violations of 18 U.S.C. § 2252A(a)(2), which makes it a crime to receive and distribute child pornography.

The statements contained in this Affidavit are based on your affiant's experience and background as a Special Agent and on information provided by other law enforcement officers.

Your affiant have been employed as a Special Agent with Homeland Security Investigations (HSI) since April of 2003, where I was assigned to the Resident Agent in Charge office in Savannah, Georgia until December of 2010, and am currently assigned to the resident Agent in Charge in Kalispell, Montana. As a Special Agent, your your affiant have participated in the investigation of a number of Federal offenses, including those identified in Title 18, United States Code, Section 2252A et seq, dealing with offenses related to child pornography. As the case Agent in several HSI investigations, your affiant have applied for federal search warrants and participated in the execution of those warrants.

Because this Affidavit is submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact known to him concerning this investigation. Your affiant has set forth only those facts which Your affiant believes are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252A are located at a residence located at 1035 2nd Avenue West, Kalispell, Montana

59901, and/or on any person located at the premises, and within a computer(s) and related peripherals, and computer media found at 1035 2nd Avenue West, Kalispell, Montana 59901.

PERTINENT CRIMINAL STATUTES

This investigation concerns alleged violations of 2252A, relating to material involving the sexual exploitation of minors.

18 U.S.C. § 2252A (a) (1) prohibits a person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

18 U.S.C. § 2252A (a) (5) (B) prohibits a person from knowingly possessing 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 in interstate or foreign commerce by any means, including by computer, or that was

produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

18 U.S.C. §2252A (a)(5) prohibits a person from knowingly accessing with the 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 in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B to this Affidavit:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (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).

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

c. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

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

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

related to or operating in conjunction with such device."

f. "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory or optical 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 and software (including, but not limited to, physical keys and locks and dongles or other electronic access devices)

g. "Computer software" as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or

other digital form. It commonly includes programs to run operating systems, applications, and utilities.

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

i. "Computer passwords and data security devices" as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, dongles, and circuit boards. Data security software of digital code 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 "booby-trap" protected data to make it inaccessible or unusable, as well

as reverse the progress to restore it.

j. "Internet Service Providers" or "ISPs" as used herein, is defined as a business that allows a user to dial into or link through its computers allowing the user to connect to the Internet for a fee. Typically, the customer pays a monthly fee and the ISP supplies software that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

k. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of

electronic communications and many other types of electronic data and files.

l. "Internet Protocol address" or "IP address", as used herein, is defined as a numeric address of a machine in the format used on the Internet. The IP address is a unique number consisting of four blocks of numbers as in 123.456.789.001, for example.

m. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, including unallocated or deleted data, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, optical, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, Personal Digital Assistants (PDAs), flash memory devices, optical disks, printer buffers, smart cards,

as well as digital data files and printouts or readouts from any magnetic, optical, electrical or electronic digital device).

n. "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: computers; central processing units; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile or cellular phones; digital cameras; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related computer communications devices such as modems, routers, network access devices, and connections; storage media such as internal and external hard drives, floppy disks, optical discs, flash memory devices, magnetic tapes; and security devices.

o. "Image" or "forensic copy" refers to an accurate reproduction of information contained on an original physical item, yet is independent of the electronic storage device.

p. A "SHA-1" is a "hash value," which derives from a mathematical algorithm that produces a numeric value that represents a specific data set.

The numeric value is an electronic fingerprint of the data and can be used to find data sets with the same hash value. It is computationally infeasible to produce a data set that corresponds to a given hash value, or to find two different data sets that produce the same hash value."

CHILD PORNOGRAPHY, COMPUTERS AND THE ONLINE EXPLOITATION OF CHILDREN

Based upon your affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom your affiant has had discussions, your affiant is aware of the following:

a. Individuals involved in the sexual exploitation of children often possess and maintain for many years records, documents and material which depict child pornography. They may receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses.

b. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation. Computers and related storage devices such as external hard drives and flash drives serve a

number of functions in connection with child pornography, to include advertisement, distribution, and storage. These devices are very small and portable. As such, they can easily be hidden in a person's residence, vehicle or on their body.

c. Child pornography is not readily available in retail establishments in the United States because it is illegal. Accordingly, individuals who wish to obtain child pornography often do so by ordering it from abroad or by discreet contact with other individuals who share their interests and have it available. The use of computers to traffic in, trade or collect child pornography has become one of the preferred methods of obtaining these materials. An individual familiar with a computer can use it in some private location to interact with another individual or a business offering such material. The use of the computer offers individuals interested in obtaining child pornography a sense of anonymity, privacy and secrecy not available elsewhere, as well as the added benefit of speedy transmissions and communications.

d. One of the most efficacious ways to expand a collection of child

pornography is to offer another collector, via a trade over the Internet, images the trading partner does not already possess. Accordingly, it may be necessary to keep a great number of images in storage so as to have adequate material to allow participation in this informal barter system. Thus, collectors involved in sending or receiving child pornography may retain it for long periods of time. This tendency is enhanced by the increased sense of security that a computer and peripherals provides. In addition to the emotional value the images have to the collector, child pornography images are intrinsically valuable to trade and/or sell and are therefore rarely destroyed or deleted by a collector. Individuals may also visit free or pay web sites, and repeatedly view child pornography images and movies that need not be saved or downloaded to their computer. Computer forensics technicians may be able to extract the images and movies that were viewed at these web sites or traded via the Internet. Individuals who procure child pornography may try to keep such material in their residence or other secure locations to ensure convenient and ready access.

e. Based on your affiant's knowledge, experience and training, your affiant believes a person utilizing a computer 1035 2nd Avenue West, Kalispell, Montana 59901, may be involved in the transportation, receipt, viewing or possession of child pornography, or the attempt to distribute, transport, receive, or possess child pornography, as evidenced by the facts set forth in this Affidavit.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers and other electronic storage devices, including electronic storage media that may contain data subject to seizure pursuant to this warrant:

Seizure and Retention of Instrumentalities

a. Based upon the foregoing, there is probable cause to believe that any computers and other electronic storage devices encountered during this search are instrumentalities of the enumerated offenses because there is probable cause to believe that they may contain contraband and fruits of crime as provided under Rule 41(c)(2), Fed. R. Crim. P., or were used in committing crime as provided under Rule 41(c)(3),

Fed. R. Crim. P. Consequently, the computers and any other electronic storage devices are subject to seizure, retention and possible forfeiture and destruction. Computers, other electronic storage devices and media confirmed onsite to contain contraband constitute fruits of crime or to have been used to commit a crime will not be returned but will be imaged offsite and analyzed as provided beginning at subparagraph (c) below. The onsite confirmation may be provided by an owner or user of the computer or storage device or, if feasible, may be obtained by conducting a limited onsite forensic examination to determine if the subject media contains any contraband or otherwise is an instrumentality. Computers and other electronic storage devices and media that are not confirmed onsite as instrumentalities will be taken offsite for imaging and preliminary analysis in accordance with subparagraph (b) below.

b. The offsite imaging and preliminary analysis of computers, other electronic storage devices and media to confirm their status as instrumentalities will be conducted within forty five (45) days of seizure. Seized items confirmed to be instrumentalities will not be returned and will be further analyzed as provided below. If the preliminary analysis, by definition an incomplete or partial analysis, does not confirm that a seized item is an instrumentality, the original item will be returned promptly to its owner, absent

an extension of time obtained from the owner or from the court. An image of the items will be retained and subjected to a complete forensic analysis, as provided below.

c. Computers and other electronic storage devices and media that are retained as instrumentalities will not be returned to its owner. The owner will be provided the name and address of a responsible official to whom the owner may apply in writing for return of specific data not otherwise subject to seizure for which the owner has a specific need. The identified official or other representative of the seizing agency will reply in writing. In the event that the owner's request is granted, arrangements will be made for a copy of the requested data to be obtained by the owner. If the request is denied, the owner will be directed to Rule 41(g), Fed. R. Crim. P.

Identification and Extraction of Relevant Data

d. A forensic image is an exact physical copy of the hard drive or other media. After obtaining a forensic image, the data will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment and software. There are literally thousands of different hardware items and software programs, and different versions of the same program, that may be

commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment may be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

e. Analyzing the contents of a computer or other electronic storage device, even without significant technical issues, may be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue: who created it; when and how it was created or downloaded or copied; when it was last accessed; when it was last modified; when it was last printed; and, when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet

applications do not store data as searchable text. The data is saved in a proprietary non-text format. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic programs but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user accessed or used other programs or services in the time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

f. It is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed, copied, uploaded or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users which

generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

g. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent of 500,000 double-spaced pages of text. Computer hard drives are

now being sold for personal computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of data also has extended the time that it takes to analyze data. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

h. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including the use of hashing tools to identify evidence subject to seizure pursuant to this warrant, and to exclude certain data from analysis, such as a known operating system and application files. The identification and extraction process may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days from the date of seizure pursuant to this warrant, absent further application to this court.

i. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION AS TO ANY CELLULAR TELEPHONE

It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "flight mode" which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some

solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

Following the issuance of this warrant, I will collect the subject cellular telephone and subject it to analysis. All forensic analysis of the data contained within the telephone and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days, absent further application to this court.

Based upon your affiant's knowledge, training, and experience, as well as information related to your affiant by investigators and others involved in the forensic examination of digital devices, your affiant knows that establishing a prospective, pre-execution search protocol in this investigation is not practical because computer searches involve a dynamic process of electronic data review and information sharing between the examining agent and agents involved in the investigation. Only after the examining agent determines the appropriate search protocol based upon his/her assessment of the specific evidence does the examining agent develop the search protocol and begin the forensic search of the digital evidence. During the course of that review, the protocol may change. Therefore, this information could not be included in a prospective, pre-execution search warrant protocol.

PEER-TO-PEER APPLICATIONS AND THE GNUTELLA NETWORK

A growing trend within the Internet is the use of peer-to-peer (P2P) file sharing programs. Through the use of P2P software Internet users are able to exchange digital files through a network of computers which are linked together via the Internet. P2P software is readily available and can be downloaded from the Internet, often for free.

P2P software generally allows users to establish files within a specific computer which can be shared with other computers running compatible P2P software. Users obtain files by opening the P2P software on their computer(s) and conducting a search for files which are currently being shared within the P2P network. File searches are conducted via search terms and the results of the searches are subsequently displayed to the user. The user then selects file(s) from the search results for download. When using LimeWire or Shareaza, popular P2P software applications, the download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

An advantage of P2P file sharing is that multiple files can be downloaded in parallel. This allows the user to download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a LimeWire or Shareaza user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this process is that it increases the speed at which a file can be downloaded. Often, however, a LimeWire or Shareaza user downloading an image file receives the entire image from one computer.

Your affiant and his office work in conjunction with the National Internet Crimes

against Children (ICAC) Task Force. Nation-wide ICAC Task Forces have been targeting individuals who are distributing child pornography via P2P file sharing applications on the Internet. Pursuant to that initiative, ICAC Task Forces members have been conducting Internet undercover operations to identify individuals using the Gnutella network and peer-to-peer software on the Internet to traffic child pornography.

Based upon your affiant's knowledge, training and experience and the experience of other law enforcement personnel, your affiant is aware that computers on the Gnutella network have software installed on them which facilitate the trading of electronic files. The software, when installed, allows users to search for pictures, movies and other digital files by entering text as search terms.

a. Gnutella network users can find images and movies containing child pornography by using search terms such as "babyj". Using the "babyj" search term usually results in the searcher being presented with a listing of files that include movies of a known pre-pubescent child victim from Georgia being vaginally penetrated by an adult male.

b. your affiant knows from training and experience, as well as the experience of other law enforcement personnel that the search results which are

presented to the user allow the user to select a file and then receive that file from other users around the world. Often these users can receive the selected file from numerous sources at once. The software can balance the network load and recover from network failures by accepting pieces of the file from different users and then reassembling the file on the local searching computer.

c. Your affiant knows from training and experience, as well as the experience of other law enforcement personnel that the Gnutella network can only succeed in reassembling a digital file from different parts and different providers if the parts all come from the exact same digital file. Your affiant knows that multiple persons sharing one file can deliver different pieces of that file to the local Gnutella compatible software and the local software can insure a complete and exact copy can be made from the parts.

d. The computer software has different methods to insure that two files are exactly the same. Your affiant knows from training and experience, as well as the experience of other law enforcement personnel that the method used by the Gnutella network involves a file encryption method called

Secure Hash Algorithm Version 1 or SHA1. Your affiant has learned that it is the Secure Hash Algorithm (SHA), developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital

Signature Standard (DSS) is specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard.

e. Digital files can be processed by the SHA1 process resulting in a digital signature. By comparing these signatures it can be concluded that two files that share the same digital signature are identical with a precision that greatly exceeds 99.9999 percent certainty. ICAC Task Force investigators have been unable to locate any documented occurrences of two different files having different contents while having the same SHA1 value.

f. Gnutella software systems use the SHA1 digital signature to uniquely identify individual files.

g. Entering search terms in Gnutella software can result in a list of SHA1 digital signatures associated with offered files. By comparing SHA1

digital signatures with signatures of known files, ICAC investigators can determine which offered files contain child pornography. ICAC Task Force investigators can then use publicly available software to request a list of Internet networked computers that are reported to have the same files for trade. This feature allows law enforcement to conduct undercover operations which involve images known to be actual and identified child pornography involving identified children.

h. Your affiant knows from training and experience, as well as the experience of other law enforcement personnel that Internet networked computers identify each other by an Internet Protocol (IP) address. These IP addresses can assist law enforcement in finding a particular computer on the Internet. IP addresses can typically lead law enforcement officers to a particular Internet service company and that company can typically identify the account which is assigned a particular IP address, at a particular date and time, to access the Internet.

i. Searching the Gnutella peer-to-peer network for files containing child pornography, as described above, can result in receiving a list of IP

addresses of computers that have Gnutella software installed. Further, the resulting list of IP addresses are of computers which have reported themselves as having available the sought after file, or portion thereof.

j. Further examination of the list of IP addresses can result in the identification of computers that are reported to be in Montana.

k. Your affiant knows from training and experience that a Globally Unique Identifier (GUID) is a pseudo-random number used in software applications. The GUID number is produced when some peer-to-peer software applications are installed on a computer and it is unique to that computer.

l. By using the above collected information, which is available to anyone using Gnutella compatible software, your affiant can conclude the following: A computer, originating from an IP address located in Montana, with Gnutella or compatible software installed, has reported to other Gnutella networked computers that it has available a file, or portion thereof, with a specific SHA1 digital signature. By comparing the advertised SHA1 digital signature with known files and their associated

SHA1 digital signature, ICAC can determine if a file, advertised for distribution contains child pornography.

m. Your affiant is aware that multiple search warrants have been executed in the State of Montana by using the above method of investigation. This method has proven to be extremely reliable in determining the location of computers that were involved in the peer-to-peer facilitated trading of child pornography. Your affiant has been involved in some of those search warrants. By using the above listed method of investigation, almost every case was verified through the following means:

1) Evidence of child pornography was found on the computer.

2) If no images of child pornography were found on the computer, interviews of persons using those computers verified that child pornography was present at one time but was deleted or the computer with the child pornography was removed from the premises.

3) Images of child pornography were moved from the computer and stored on other media.

DETAILS OF THE INVESTIGATION

On January 13, 2015 at 0048 (UTC-07:00), Detective Jeanne Parker with Flathead County Sheriffs Office, in Kalispell, Montana, using the E-Phex software, established a direct connection with a computer at IP address 184.166.178.106 and a files list was obtained from the shared folder. Detective Parker established a connection with the same IP address. The files list showed changes in the number and/or content of files matching suspected child pornography hash values contained in the local SHA-1 database since the last time E-Phex successfully browsed the shared folder of the computer at IP address 184.166.178.106.

On January 13, 2015 at 0048 (UTC-07:00), Detective Parker attempted to obtain a list of files reported as being shared on the Gnutella by the computer at IP address 184.166.178.106. The computer at IP address 184.166.178.106 reported 10 files being shared on the Gnutella, of which 2 files were investigative files of interest. Below are the 2 filenames and SHA-1 values.

File Name	SHA-1
13yo Vera 15yo Olga get cum in face (two 13yo little girls cumshot facial pthc pedo jailbait preteen r@ygold hussyfan 12yo 16yo).mpg	XQX4GBE2RXJ5QMIIBUZTLAMLQ2ZP2E34

(Pthc) (Webcam) Blonde%26Bf 14 Yr Old Jacking Off To Preteen Lolita Pussy Then Cumin On Stomach Sex Rape Russian Incest Underage Dick Boy Girl Cum Mpg(4).mpg	TUAEKEUQO5AV6MNJKUJN6QI7FC7NIUBG

On January 13, 2015, while directly connected to the computer at IP address 184.166.178.106, Detective Parker captured the GUID associated to the peer to peer program operating on that computer. The program is reporting itself as Turbo Wire/4.0.0. The GUID is as follows: 78B34E24782E9DA9C596518ECF41C700.

On January 13, 2015, Detective Parker conducted a query on the IP address 184.166.178.106 through the American Registry for Internet Numbers (ARIN). ARIN reported IP address 184.166.178.106 to be registered to Charter Communications.

On January 13, 2015 at 0116 (UTC-07:00), Detective Parker again obtained a list of files reported as being shared on the network from the computer at IP address 184.166.178.106. The file list showed changes in the number and/or content of the investigative files of interest. The file list contained 24 files of which 10 files were investigative files of interest below are the 10 filenames and SHA-1 values.

File Name	SHA-1
13yo Vera 15yo Olga get cum in face (two 13yo little girls cumshot facial pthc pedo jailbait preteen r@ygold hussyfan 12yo 16yo).mpg	XQX4GBE2RXJ5QMIIBUZTLAMLQ2ZP2E34
(Pthc) (Webcam) Blonde%26Bf 14 Yr Old Jacking Off To Preteen Lolita Pussy Then Cumin On Stomach Sex Rape Russian	TUAEKEUQO5AV6MNJKUJN6QI7FC7NIUBG

Incest Underage Dick Boy Girl Cum Mpg(4).mpg	
(~pthc center~)(opva)(2013) brazil blonde 8yr girl spycam slit and panties.avi	65XQY4TFD5YLRBWWY6PNYOWADM6Y2NGK
(pthc,pedo,preteen)_11yo Tonya shows tits and pussy(rus)(no sound).avi	KZTKHUTQOWJIVFATF42PQSC4RP5D6Y76
Pthc 2012 - 11Yo Katerin Turismo Pussy Fuck (Venezuela) Preteen,Loli,Bibcam,Ptsc,New,Cum,9Yo,10Yo.avi	U6CAGM7TDW3P7YJCXSEHOA3QELXFXRIE
Pthc - Hmm Gracel Series - Lea Set 3 Complete Fuck - 3m24s.mpg	RGDLTWIRBUKBMBKYS5HCXXZTQ2UK4YQP
(PTHC) BEST! HARD 7yo child abusive sex - PORN.mpg	QQ4CQNK5HG2IAAYHW3MRWZ2GFI5J4JRF
13yr + sis(Hussyfan) (pthc) (r@ygold) (babyshivid) 109 Pedofilia 13yr dad.mpg	CTOSIVKLQZQYLTHWP7HZV7LTVLYO6SOK
Webcam pthc - Alex part 10yo girl vaginal fucked.avi	TERYN47HRE6V2QAN3HQ63LWISMMWZ43I
(~Pthc Center~)(Opva)(2014) Dad-Daughter e085-Chinese Girls Serie.avi	WORRVQPHDA4COL43PRDVEWJCQ5L4YDMF

On January 13, 2015 at 0157 (UTC-07:00), Detective Parker again obtained a list of files reported as being shared on the network from the computer at IP address 184.166.178.106. The file list showed changes in the number and/or content of the investigative files of interest. The file list contained 26 files of which 12 files were investigative files of interest below is a sampling of 10 filenames and their SHA-1 values.

File Name	SHA-1
13yo Vera 15yo Olga get cum in face (two 13yo little girls cumshot facial pthc pedo jailbait preteen r@ygold hussyfan 12yo 16yo).mpg	XQX4GBE2RXJ5QMIIBUZTLAMLQ2ZP2E34
(Pthc) (Webcam) Blonde%26Bf 14 Yr Old Jacking Off To Preteen Lolita Pussy Then Cumin On Stomach Sex Rape Russian Incest Underage Dick Boy Girl Cum Mpg(4).mpg	TUAEKEUQO5AV6MNJKUJN6QI7FC7NIUBG
(~pthc center~)(opva)(2013) brazil blonde 8yr girl	65XQY4TFD5YLRBWWY6PNYOWADM6Y2NGK

spycam slit and panties.avi	
(pthc,pedo,preteen) 11yo Tonya shows tits and pussy(rus)(no sound).avi	KZTKHUTQOWJIVFATF42PQSC4RP5D6Y76
Pthc 2012 - 11Yo Katerin Turismo Pussy Fuck (Venezuela) Preteen,Loli,Bibcam,Ptsc,New,Cum,9Yo,10Yo.avi	U6CAGM7TDW3P7YJCXSEHOA3QELXFXRIE
Pthc - Hmm Gracel Series - Lea Set 3 Complete Fuck - 3m24s.mpg	RGDLTWIRBUKBMBKYS5HCXXZTQ2UK4YQP
(PTHC) BEST! HARD 7yo child abusive sex - PORN.mpg	QQ4CQNK5HG2IAAYHW3MRWZ2GFI5J4JRF
13yr + sis(Hussyfan) (pthc) (r@ygold) (babyshivid) 109 Pedofilia 13yr dad.mpg	CTOSIVKLQZQYLTHWP7HZV7LTVLYO6SOK
Webcam pthc - Alex part 10yo girl vaginal fucked.avi	TERYN47HRE6V2QAN3HQ63LWISMMWZ43I
(~Pthc Center~)(Opva)(2014) Dad-Daughter e085-Chinese Girls Serie.avi	WORRVQPHDA4COL43PRDVEWJCQ5L4YDMF

On January 13, 2015 at 0240 (UTC-07:00), Detective Parker again obtained a list of files reported as being shared on the network from the computer at IP address 184.166.178.106. The file list showed changes in the number and/or content of the investigative files of interest. The file list contained 48 files of which 22 files were investigative files of interest. below is a sampling of 10 filenames and their SHA-1 values.

File Name	SHA-1
13yo Vera 15yo Olga get cum in face (two 13yo little girls cumshot facial pthc pedo jailbait preteen r@ygold hussyfan 12yo 16yo).mpg	XQX4GBE2RXJ5QMIIBUZTLAMLQ2ZP2E34
(Pthc) (Webcam) Blonde%26Bf 14 Yr Old Jacking Off To Preteen Lolita Pussy Then Cumin On Stomach Sex Rape Russian Incest Underage Dick Boy Girl Cum Mpg(4).mpg	TUAEKEUQO5AV6MNJKUJN6QI7FC7NIUBG

(~pthc center~)(opva)(2013) brazil blonde 8yr girl spycam slit and panties.avi	65XQY4TFD5YLRBWWY6PNYOWADM6Y2NGK
(pthc,pedo,preteen)_11yo Tonya shows tits and pussy(rus)(no sound).avi	KZTKHUTQOWJIVFATF42PQSC4RP5D6Y76
Pthc 2012 - 11Yo Katerin Turismo Pussy Fuck (Venezuela) Preteen,Loli,Bibcam,Ptsc,New,Cum,9Yo,10Yo.avi	U6CAGM7TDW3P7YJCXSEHOA3QELXFXRIE
Pthc - Hmm Gracel Series - Lea Set 3 Complete Fuck - 3m24s.mpg	RGDLTWIRBUKBMBKYS5HCXXZTQ2UK4YQP
(PTHC) BEST! HARD 7yo child abusive sex - PORN.mpg	QQ4CQNK5HG2IAAYHW3MRWZ2GFI5J4JRF
13yr + sis(Hussyfan) (pthc) (r@ygold) (babyshivid) 109 Pedofilia 13yr dad.mpg	CTOSIVKLQZQYLTHWP7HZV7LTVLYO6SOK
Webcam pthc - Alex part 10yo girl vaginal fucked.avi	TERYN47HRE6V2QAN3HQ63LWISMMWZ43I
(~Pthc Center~)(Opva)(2014) Dad-Daughter e085-Chinese Girls Serie.avi	WORRVQPHDA4COL43PRDVEWJCQ5L4YDMF

On January 14, 2015, an investigative subpoena (ICE-HSI-KM-2015-00019) was served by your affiant on the Internet Service Provider (ISP), Charter Communications the listed owner of assigned IP address 184.166.178.106. The subpoena requested the identification of the subscriber using IP address 184.166.178.106.

On January 21, 2015, a 2008 silver in color Forester Subaru, displaying Montana tag number 7C5220A was stopped by the Kalispell Police Department for a traffic violation. The vehicle was driven by Rodney Dean STELL; the vehicle is currently registered to Rodney STELL at 1035 2nd Avenue West Kalispell, Montana 59901, in Flathead County

On January 23, 3015, Charter Communications provided the following in response

to the subpoena (ICE-HSI-KM-2015-00019) on the subscriber of the IP address 184.166.178.106:

Name:	Rodney STELL
Address:	1035 2nd Avenue West Kalispell, Montana 59901 Flathead County
Telephone:	Never Connected / internet only
E-mail address:	Unknown
Account date:	for IP address 06/04/2012 to present

On January 23, 2015, as part of the above response, Charter Communication was able to verify that IP address 184.166.178.106 was assigned to Rodney STELL from June 04, 2012 to present time.

Commercial databases indicated Rodney STELL is associated with the address 1035 2nd Avenue West Kalispell, Montana 59901, Flathead County.

On January 27, 2015, your affiant located and photographed the residence belonging to Rodney Dean STELL at 1035 2nd Avenue West Kalispell, Montana 59901. Your affiant searched the area for unsecured wireless internet around the address of 1035 2nd Avenue West Kalispell, Montana 59901. The only unsecured wireless internet was public Wi-Fi belonging to Flathead County.

On January 27, 2015, your affiant conferred with Detective Earl Campbell with

the Great Falls Police Department, in Great Falls Montana, and a member of the Montana Internet Crimes against Children Task Force. The five files bellow are samples of the files being reported as being shared on the network from the computer at IP address 184.166.178.106, as listed above.

CTOSIVKLQZQYLTHWP7HZV7LTVLYO6SOK
Age Difficult
This video file is approximately 1 minute and 49 seconds and depicts a nude adult male having vaginal intercourse with two nude juvenile females, at different times. One is lying on her back and the other is on her knees and elbows. All sexual acts depicted in this video appear to depict the same adult male on the same bed. Both females appear to be under the age of 18

QQ4CQNK5HG2IAAYHW3MRWZ2GFI5J4JRF
Child Notable
This video file is approximately 1 minute and 41 seconds in length and depicts a prepubescent female lying on her back being vaginally penetrated by an adult male's penis.

TERYN47HRE6V2QAN3HQ63LWISMMWZ43I
Child Notable
This video file is approximately 16 minutes and 52 seconds in length and depicts a naked prepubescent girl sitting on a metal chair. She walks away and a naked adult male sits in the chair. The male then has vaginal sex with the child. The girl has no pubic hair and no breasts. This is a very low quality video and very "choppy" when playing.

U6CAGM7TDW3P7YJCXSEHOA3QELXFXRIE
Child Notable
This video file is approximately 2 minutes and 46 seconds in length and depicts a bottomless prepubescent girl wearing a pink shirt and lying on her back. A man is placing his erect penis in the girl's vagina. The video moves up and down the child's body zooming in and out on the child's vagina, face, and nipples. The video also at one point shows a laptop computer that is playing a pornographic video on a counter next to the child.
XQX4GBE2RXJ5QMIIBUZTLAMLQ2ZP2E34
Child Notable
This video file is approximately 41 seconds in length and depicts two nude juvenile females kissing while an adult male masturbates. The adult male then ejaculates onto the female's faces.

CONCLUSION

Based on the foregoing, there is probable cause to believe that Title 18 U.S.C. § 2252A, which, among other things, make it a federal crime for any person to view, possess, receive or distribute child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at 1035 2nd Avenue West Kalispell, Montana 59901, Flathead County, or any person found at the premises, as more fully described in Attachment A.

Respectfully submitted,

Richard McManaway, Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 3rd day of ~~January~~ February 2015

United States Magistrate Judge Jeremiah C. Lynch