

AO 91 (Rev. 11/11) Criminal Complaint

## UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America  
v.  
KURT BATUCAN SHELTON

Case No.

3:20-mj-1297-JRK

Defendant(s)

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2020, and September 4, 2020 in the county of Putnam in the  
Middle District of Florida, the defendant(s) violated:

## Code Section

18 U.S.C. § 2251(a)  
18 U.S.C. § 2252(a)(4)

## Offense Description

Production of child pornography  
Possession of a visual depiction the production of which involved the use of a  
minor engaging in sexually explicit conduct

This criminal complaint is based on these facts:

See attached affidavit.

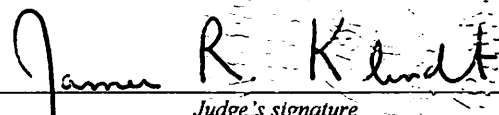
☒ Continued on the attached sheet.


Complainant's signature

Benjamin J. Luedke, HSI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 9-4-2020City and state: Jacksonville, Florida


Judge's signature

JAMES R. KLINDT, United States Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF COMPLAINT**

I, Benjamin J. Luedke, being duly sworn, state as follows:

1. I am a Special Agent (S/A) with Homeland Security Investigations (HSI), the investigative arm of Immigration and Customs Enforcement (ICE), formerly known as the United States Customs Service. I have been assigned to the Office of the Assistant Special Agent in Charge, Jacksonville, Florida since August 2007. Prior to that, I was assigned to the Blaine, Washington office, beginning in July of 2002. I am a law enforcement officer of the United States and am thus authorized by law to engage in or supervise the prevention, detection, investigation or prosecution of violations of federal criminal law. I am responsible for enforcing federal criminal statutes under the jurisdiction of HSI, including violations of law involving the exploitation of children. I have attended the Basic Criminal Investigator School and the United States Immigration and Customs Enforcement Academy at the Federal Law Enforcement Training Center in Brunswick, Georgia, and I have received training in the area of Customs laws. In my capacity as a Special Agent, I have participated in numerous types of investigations during which I have conducted or participated in physical surveillance, undercover transactions and operations, historical investigations, extradition cases and other complex investigations. Prior to my employment with HSI, I worked as a federal police officer with the U.S. Capitol Police from June 2000 to March 2002. Since becoming a

JRK

Special Agent, I have worked with experienced Special Agents and state and local law enforcement officers who also investigate child exploitation offenses.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2423, as well as Florida state statutes that criminalize sexual activity with minors and other methods of child sexual exploitation. In connection with such investigations, I have served as case agent and have served as an undercover agent in online child exploitation cases. During the course of my investigations, I have worked closely with members of the local child exploitation task force comprised of agents and officers from HSI, the Federal Bureau of Investigation (FBI), the Florida Department of Law Enforcement (FDLE), the Jacksonville Sheriff's Office (JSO), the St. Johns County Sheriff's Office (SJSO), and the Clay County Sheriff's Office (CCSO), among other agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. 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. This affidavit is being submitted for the limited purpose of establishing

probable cause for the filing of a criminal complaint, 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 that Kurt Batucan SHELDON has committed violations of 18 U.S.C. § 2251(a) (sexual exploitation of children - producing child pornography) and 18 U.S.C. § 2252(a)(4) (possession of child pornography).

4. This affidavit is made in support of a complaint against Kurt Batucan SHELDON, that is, in Putnam County, in the Middle District of Florida, and elsewhere, in or about May 2020, SHELDON did knowingly employ, use, persuade, induce, entice, and coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of the conduct knowing and having reason to know that such visual depiction would be transported and transmitted using any means and facility of interstate and foreign commerce, in violation of 18 U.S.C. § 2251(a); and, on or about September 4, 2020, SHELDON did knowingly possess a matter that contained visual depictions that had been produced using materials that had been shipped and transported in and affecting interstate and foreign commerce, by an means, when the production of which involved the use of a prepubescent minor engaging in sexually explicit conduct, and the visual depiction was of such conduct, in violation of 18 U.S.C. § 2252(a)(4).

5. On September 2, 2020, I applied for and obtained a federal search

warrant for the premises located at 230/232 Ofarrell Avenue, Interlachen, Florida 32148, which I believed to be occupied by SHELDON, among others, and a copy of which is attached hereto as Exhibit 1, and the facts and information contained therein are hereby incorporated by reference.

6. On September 4, 2020, HSI Jacksonville Special Agents, along with Putnam County Sheriff's Office (PCSO) Deputies and Detectives, executed the aforementioned search warrant at approximately 6:00 a.m. at 230/232 Ofarrell Avenue, Interlachen, Florida 32148.

7. During the search of SHELDON's bedroom, HSI special agents discovered a 256GB SanDisk Cruzer Glide thumb drive inserted in a homemade computer. The computer was on a stand adjacent to SHELDON's bed. I have viewed the SanDisk Cruzer Glide thumb drive and it states that it was made in China.

8. A preliminary examination of the SanDisk Cruzer Glide thumb drive conducted on scene by HSI Computer Forensic Analysts (CFA) James Greenmun and Antonio Contes during the execution of the search warrant revealed multiple video and still image files of child pornography resident on the SanDisk Cruzer Glide thumb drive. One such file that I have reviewed and has a create date of August 15, 2017, that was resident on the SanDisk Cruzer Glide thumb drive is described as follows:

DESCRIPTION: This is a color .gif video file. The video depicts a completely nude prepubescent female child standing next to a bed. A completely nude adult male is standing in front of her and has one leg on the bed. The child is manually stimulating the male's erect penis with one of her hands. I believe she is a young child based upon her child-like facial features, lack of breast development, lack of pubic hair, and overall body size.

Based on my training and experience, I believe the file depicts at least one minor engaged in sexually explicit conduct, and therefore constitutes child pornography pursuant to 18 U.S.C. § 2256. A second file that I have reviewed and has a create date of August 15, 2017, that was also resident on the SanDisk Cruzer Glide thumb drive, is described as follows:

DESCRIPTION: This is a color image and it depicts a completely nude prepubescent female child sitting on the lap of another female, who is sitting on a chair. The child's legs are spread, thereby exposing her bare vagina. The other female is spreading the child's vagina open with her hands. I believe she is a young child based upon her child-like facial features, lack of breast development, lack of pubic hair, and overall body size.

Based on my training and experience, I believe the file depicts at least one minor engaged in sexually explicit conduct, and therefore constitutes child pornography pursuant to 18 U.S.C. § 2256.

9. PCSO Det. Gentry and I made contact with SHELDON. After being advised of and waiving his *Miranda* rights, SHELDON agreed to speak with us. I recorded the interview. Among other things, SHELDON provided the following information:

SHELDON acknowledged that the 256GB SanDisk Cruzer Glide thumb drive and homemade computer in his bedroom belonged to him. SHELDON acknowledged that there would be child sexual abuse material (CSAM) on his computer. SHELDON acknowledged using the DarkWeb to search for CSAM. SHELDON acknowledged receiving CSAM from “teens” via Snapchat. SHELDON admitted that he would ask girls he met on online applications who he knew to be underage to send him nude photographs “a couple of times.” SHELDON acknowledged requesting from a fifteen (15) year old female, images of her vagina, of her sexually posing, and of her inserting an object into her vagina. SHELDON acknowledged similar activity with other underage females as well. SHELDON acknowledged he is sexually attracted to children and masturbates while viewing CSAM.

### CONCLUSION

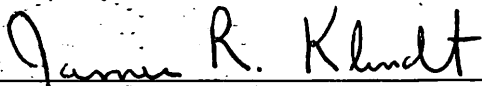
10. Based upon the foregoing facts, and including those facts set forth in Exhibit 1, I have probable cause to believe that, in Putnam County, in the Middle District of Florida, and elsewhere, in or about May 2020, SHELDON did knowingly employ, use, persuade, induce, entice, and coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of the conduct knowing and having reason to know that such visual depiction would be transported and transmitted using any means and facility of interstate and foreign commerce, in

violation of 18 U.S.C. § 2251(a); and, on or about September 4, 2020, SHELDON did knowingly possess a matter that contained visual depictions that had been produced using materials that had been shipped and transported in and affecting interstate and foreign commerce, by an means, when the production of which involved the use of a prepubescent minor engaging in sexually explicit conduct, and the visual depiction was of such conduct, in violation of 18 U.S.C. § 2252(a)(4).



Benjamin J. Luedke, Special Agent  
Homeland Security Investigations

Sworn to before me this  
this 4<sup>th</sup> day of September, 2020



JAMES R. KLINDT  
United States Magistrate Judge

# EXHIBIT 1

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

# 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)

The premises located at 230/232 Ofarrell Avenue,  
Interlachen, FL 32148, as further described in  
Attachment A

Case No. 3:20-mj- 1290-JRK

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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):

the premises located at 230/232 Ofarrell Avenue, Interlachen, FL 32148, as further 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:

Code Section	Offense Description
18 U.S.C. §§ 2252 & 2252A	Possession, receipt, transportation and distribution of child exploitation material

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.

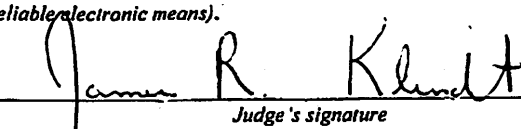
  
Applicant's signature

Benjamin Luedke, HSI Special Agent  
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
and 41(d)(3) over the telephone. (specify reliable electronic means).

Date: 9-2-2020

City and state: Jacksonville, Florida

  
Judge's signature

James R. Klindt, United States Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, Benjamin J. Luedke, being duly sworn, hereby state as follows:

1. I am a Special Agent (S/A) with Homeland Security Investigations (HSI), the investigative arm of Immigration and Customs Enforcement (ICE), formerly known as the United States Customs Service. I have been assigned to the Office of the Assistant Special Agent in Charge, Jacksonville, Florida since August 2007. Prior to that, I was assigned to the Blaine, Washington office, beginning in July of 2002. I am a law enforcement officer of the United States and am thus authorized by law to engage in or supervise the prevention, detection, investigation or prosecution of violations of federal criminal law. I am responsible for enforcing federal criminal statutes under the jurisdiction of HSI, including violations of law involving the exploitation of children. I have attended the Basic Criminal Investigator School and the United States Immigration and Customs Enforcement Academy at the Federal Law Enforcement Training Center in Brunswick, Georgia, and I have received training in the area of Customs laws. In my capacity as a Special Agent, I have participated in numerous types of investigations during which I have conducted or participated in physical surveillance, undercover transactions and operations, historical investigations, extradition cases and other complex investigations. Prior to my employment with HSI, I worked as a federal police officer with the U.S. Capitol Police from June 2000 to March 2002. Since becoming a Special Agent, I have worked with experienced Special Agents and state and local law enforcement

JRK

officers who also investigate child exploitation offenses.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2423, as well as Florida state statutes that criminalize sexual activity with minors and other methods of child sexual exploitation. In connection with such investigations, I have served as case agent and have served as an undercover agent in online child exploitation cases. During the course of my investigations, I have worked closely with members of the local child exploitation task force comprised of agents and officers from HSI, the Federal Bureau of Investigation (FBI), the Florida Department of Law Enforcement (FDLE), the Jacksonville Sheriff's Office (JSO), the St. Johns County Sheriff's Office (SJSO), and the Clay County Sheriff's Office (CCSO), among other agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. This affidavit is based upon my personal knowledge, experience and training, as well as other information developed during this investigation. Because this affidavit is being submitted for the limited purpose of establishing probable cause and securing a search warrant, 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 that contraband, fruits, instrumentalities, other items illegally possessed and evidence of violations of 18 U.S.C. §§ 2252 and/or 2252A, are present in the location to be searched.

4. I make this affidavit in support of an application for a search warrant for authority to search the premises located at 230 and 232 Ofarrell Avenue, Interlachen, FL 32148 (the "Subject Location") as more particularly described in Attachment A, which include multiple trailers, an additional large structure, and multiple sheds, as well as any computer and computer media and electronic storage devices located therein. I also request to seize any and all items listed in Attachment B as evidence, fruits, and instrumentalities of criminal activity specified herein.

#### **STATUTORY AUTHORITY**

5. This investigation concerns alleged violations of 18 U.S.C. §§ 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, computer forensic examiners, and federal prosecutors, 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 mails.

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, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, or have been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which were 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.

### **DEFINITIONS**

6. 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 process 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) may assign a unique and different number to a computer at different times that 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.

k. "Wireless telephone" (or mobile telephone, or cellular telephone, or smart phone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually

contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Many wireless telephones are minicomputers or "smart phones" with immense storage capacity.

l. A "digital camera" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

m. A portable media player (or "MP3 Player" or iPod) is a

handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

#### **COMPUTERS AND CHILD PORNOGRAPHY**

7. 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.

JRK

8. 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.

9. 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, as well as “smart” phones, 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.

10. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, 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.

11. The World Wide Web of the Internet, and especially the dark web, affords collectors of child pornography several different venues for obtaining,

viewing and trading child pornography in a relatively secure and anonymous fashion.

12. 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.

13. 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

JRK

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 can record communication in transcript form, often 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 peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

#### **SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

14. 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, 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. 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.

#### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

15. 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 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, Peer-to-Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Some 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. Some 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 devices using the Internet often maintain and/or possess the items listed in Attachment B.

16. 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 learned from HSI S/A Algozzini that he conducted an investigation in 2016 in the Middle District of Florida in which the subject had his residence searched in July 2016 pursuant to a state search warrant and his wireless telephone and computer tablet seized by the Jacksonville Sheriff's Office. The search of these devices revealed the subject knowingly possessed several images of child pornography. The subject retained an attorney, and both were made aware of the ongoing investigation into the subject's commission of child pornography offenses. Approximately two months later, the subject was arrested on federal child pornography charges. On the same day as the subject's arrest, HSI executed a federal search warrant and seized a wireless telephone acquired and used by the subject after the execution of the state search warrant at his residence. Subsequent forensic examination of this wireless telephone revealed that the subject had received, possessed and viewed images of child pornography numerous times on his new device after the execution of the state search warrant and before his federal arrest.

17. 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 favorite images involving a particular child or act is often maintained on the device.

18. Based on my training and experience, I know that within the last several years, individuals who have a sexual interest in minor children have used the Internet and Internet-enabled devices with increasing frequency to make contact with and attempt to establish relationships with potential child victims. These individuals may perceive that the internet provides some degree of anonymity and safety from prosecution. Because more and more children are using the Internet and Internet enabled devices, these individuals potentially expose more and more child victims to online sexual exploitation. These individuals may contact potential child victims through social networking websites such as Facebook and Twitter or may engage in online conversations with children through text messaging and email. During these online conversations, photographic images and links to Internet websites can be easily

exchanged between the individual and the targeted child. Based on my training and experience, I know that when such an individual uses text messaging, email, or other websites to have online contact with children, the Internet-enabled device used, whether it is a computer, a wireless telephone, a “smart” phone or a tablet such as an “iPad,” often saves and maintains evidence of such contacts. This evidence can often be extracted and examined by a trained forensic examiner.

### **BITTORRENT PEER TO PEER FILE SHARING**

19. Based on my training and experience, I know the following regarding Peer to Peer (hereinafter referred to as “P2P”) file sharing networks, P2P client software programs, and the BitTorrent P2P file-sharing network.

20. A phenomenon on the Internet is P2P file sharing. P2P file sharing is a method of communication available to Internet users through using special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file-sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network. Additionally, a particular P2P client software program

may be able to access multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. The user interface features, and configurations may vary between clients and versions of the same client.

21. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file-sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file-sharing network.

22. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Settings within these programs control sharing thresholds.

23. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

24. Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for

distribution to other P2P clients. In some clients, individual files can also be shared.

25. Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

26. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

27. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the

segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

28. P2P file-sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

29. The BitTorrent network is a very popular and publically available P2P file-sharing network. Most computers that are part of this network are referred to as "peers." The terms "peers" and "clients" can be used interchangeably when referring to the BitTorrent network. A peer can simultaneously provide files to some peers while downloading files from other peers.

30. The BitTorrent network can be accessed by computers running many different client programs, some of which include the BitTorrent client program, uTorrent client program, and Vuze client program. These client programs are publically available and free P2P client software programs that can be downloaded from the Internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interface features and configuration may vary between clients and versions of the same client.

31. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to

share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent network users to download.

32. In order to share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A "Torrent" is typically a small file that describes the file(s) that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but information about the file(s) described in the "Torrent," such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash" is a SHA-1<sup>1</sup> hash value of the set of data describing the file(s) referred to in the "Torrent," which include the SHA-1 hash value of each file piece, the file size, and the file name(s). The

---

<sup>1</sup> SHA-1, or Secure Hash Algorithm Version 1, is a file encryption method which may be used to produce a unique digital signature of a file. Finding a file that produces the same SHA-1 value as a known file requires a search and comparison of  $10^{48}$  ( $2^{160}$ ) different files, which is computationally infeasible. The Secure Hash Algorithm (SHA) was 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) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard.

"info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referred to in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referred to in the "Torrent." It is important to note that the "Trackers" do not actually have the file(s) and are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

33. Once a torrent is created, in order to share the file(s) referenced in the "Torrent" file, a user typically makes the "Torrent" available to other users, such as via websites on the Internet.

34. In order to locate "Torrent" files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on websites hosting "Torrents." Once a "Torrent" file is located that meets the keyword search criteria, the user will download the "Torrent" file to their computer. Alternatively, a user can also search for and locate "magnet links," which is a

link that enables the BitTorrent network client program itself to download the "Torrent" to the computer. In either case, a "Torrent" file is downloaded to the user's computer. The BitTorrent network client will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referred to in the "Torrent," to include the remote peers/clients Internet Protocol (IP) addresses.<sup>2</sup>

35. For example, a person interested in obtaining child pornographic images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." (It should be noted that this situation did not occur in this investigation.) The results of the torrent search are typically returned to the user's computer by displaying them on the torrent-hosting website. The hosting website

---

<sup>2</sup> Computers on the Internet identify each other by an Internet Protocol or IP address. IP addresses can assist law enforcement in finding a particular computer on the Internet. IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account and location that used the IP address to access the Internet.

will typically display information about the torrent, which can include the name of the torrent file, the name of the file(s) referred to in the torrent file, the file(s) size, and the "info hash" SHA-1 value of the torrent file. The user then selects a torrent of interest to download to his or her computer. Typically, the BitTorrent client program will then process the torrent file. The user selects from the results displaying the file(s) he or she wants to download that were referred to in the torrent file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referred to in the torrent file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referred to in the torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or the client program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

36. Typically, as described above, one method for investigators to search the BitTorrent network for users possessing and/or disseminating child pornography files is to type in search terms, based on their training and experience, that would return a torrent filename indicative of child pornography. The investigator would then download the file(s) referred to within the torrent file and determine if the file(s) indeed contained child pornography. If so, the investigator can document the "info hash" SHA-1 hash value of this torrent file, to be compared with future identical torrent files observed on the BitTorrent network. Although transparent to the typical user, when searches are conducted, additional results are received from the trackers on other peers who recently reported to the network as having that file(s) in whole or in part, which may include the IP addresses of those peers/clients. This information can be documented by investigators and compared to those "info hash" SHA-1 hash values the investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the "info hash" SHA-1 hash value and determine with mathematical certainty that a file seen on the network is an identical copy of a child pornography file he or she has seen before.

37. The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the

approximate location of these IP addresses is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, an association between a known torrent file (based upon on the “info hash” SHA-1 hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

38. Once a client user is identified as recently having a file believed to be child pornography, in whole or in part, the investigator can then query that client user directly to confirm that the client user has that file, in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single-source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either. The process of sharing files on the BitTorrent network involves peers allowing other peers to copy a file or portions of a file. This sharing process does not remove the file from the computer sharing the file. This process places a copy of the file on the computer that downloaded it.

39. If an investigator either received an affirmative response from a remote peer that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote peer at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running a BitTorrent network P2P

client and is currently possessing, receiving, and/or distributing specific and known visual depictions of child pornography.

40. Law enforcement has created BitTorrent network client programs that obtain information from "Trackers" about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the "info hash" SHA-1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network). This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network.

41. During the query and/or downloading process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading a file from. This information can include (1) the remote client's IP address; (2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the remote client program; and (3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

42. The investigation of peer-to-peer 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 Task Force Program. 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 the sexual exploitation of actual child victims.

43. Computers throughout the world can download files from download candidates without regard to geographic location. I know that the files located on P2P download candidates are quickly available throughout the world due to the distributed sharing model of P2P networks.

44. 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.

**FACTS ESTABLISHING PROBABLE CAUSE**

45. I make this affidavit in support of a search warrant for the Subject Location I believe to be currently occupied by Kurt Batucan Sheldon, Dustin Sheldon, Dwight Sheldon, and several other family members. This affidavit is based upon information provided to me both verbally and in written documentation from other law enforcement officers and personnel, to include Clay County Sheriff's Office (CCSO) Detective (Det.) Ryan Ellis, and Saint Johns County Sheriff's Office (SJSO) Det. Kevin Greene, as well as through an investigation that I personally conducted as set forth herein. I have personally observed the Subject Location, and it appears as set forth in Attachment A. In addition, I requested and was subsequently provided with aerial images of the premises taken by Customs and Border Protection (CBO) Officers on August 20, 2020, and the images confirm, while providing a broader and more specific view, what I have personally observed during ground surveillance on multiple occasions. Specifically, the aerial photos confirmed there are two trailers, an additional large structure, and multiple sheds on the property.

46. HSI is investigating the use of one or more computers, wireless telephones, and computer media at the Subject Location to commit violations of 18 U.S.C. §§ 2252 and 2252A, which prohibit the transportation, receipt, distribution, possession, and access with intent to view child pornography, that

is, visual depictions of one or more minors engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256.

47. During August 2020, I learned from Det. Ellis that in May 2020, he initiated an investigation related to a report of inappropriate sexual messages between a minor and an adult via Snapchat, a popular chat application.

48. Based on my communication with Det. Ellis, and my review of reports and documents provided by Det. Ellis, I have learned the following, among other things:

a. On May 27, 2020, CCSO Deputy G. Ehrenfeld, in response to a call for service, contacted the mother and father of a 12-year-old minor, herein referred to as Minor Victim 1 (MV1). The parents of MV1 informed Deputy Ehrenfeld they discovered that MV1 had been sending and receiving sexually explicit messages from an individual they believed to be an adult male. The parents of MV1 advised the messages included pictures and videos sent by MV1. MV1 and her parents provided the following information to Deputy Ehrenfeld, and Deputy Ehrenfeld prepared a report that I have reviewed:

MV1 advised that she began communicating with an unknown person using the screen name "K.T." (later confirmed as "K t") approximately three weeks ago. MV1 advised she posted something about wanting friends on the Whisper application and "K t" responded. MV1 advised they started a conversation and MV1 told him she was almost sixteen (16). MV1 advised that

"K t" was represented as a male and 25-29 years of age on Whisper. MV1 advised the conversations were friendly and then progressed to the point in which MV1 sent him a picture of herself, and "K t" sent one of himself. MV1 advised that she and "K t" continued messaging and the communication became sexual in nature. MV1 advised "K t" convinced her to send more risqué pictures of herself to him. MV1 advised she and "K t" then began messaging via Snapchat. MV1 advised she sent some pictures to "K t" in bikinis and underwear and he continued to compliment her, and he requested that she send him pictures and videos of her naked and masturbating. MV1 advised she sent approximately fifty (50) images and/or videos of her naked and/or touching herself from her iPhone 8+ phone. MV1's mother signed a Voluntary Consent to Search Form for the iPhone 8+ phone. Deputy Ehrenfeld then transported the iPhone 8+ phone to the CCSO ICAC Unit and submitted it into evidence.

b. On May 28, 2020, Det. Ellis spoke with MV1's mother who advised that the person communicating with a screen name of "K t" via Snapchat has a username of "tacticfallout." In my training and experience, I know that Snapchat has a function that allows users to display a screen name different from their username to display a name of their choice. MV1's mother was able to figure out "K t's" username based on the Snapchat profile within MV1's phone for "K t." I have since reviewed MV1's phone and Snapchat application and confirmed the same. MV1's mother advised that "K t" told MV1 he lives in "Putnam." MV1's mother provided Det. Ellis with several screen

shots of Snapchat communication between MV1 and “K t.” In the Snapchat screenshots, “K t” engages in a series of sexually explicit conversations with MV1 and also makes comments that appear to acknowledge the receipt of child exploitation material. “K t” asks for more images from MV1. Det. Ellis provided me with copies of the screen shots, and I have reviewed them. A sample of messages sent from “K t” to MV1 is as follows:

“Maybe you should strip if you’re still bothered and turned on kitty”

“Squeeze your boobs together and open your mouth for daddy. I want to see your whole face when you do”

“Glad you enjoyed telling daddy that [two monkey emojis]  
Plus that smirk and that wink...fuck baby  
I wouldn’t think you’ve never seen or sucked a cock”

“Still too shy huh  
Hmmm well find a brush to pretend it’s daddy’s cock  
And show him what you’d do”

“I wish I could sneak you out [monkey covering eyes emoji]

“Mmm suck that brush while you finger and play with yourself”

c. On May 29, 2020, Det. Ellis reviewed the forensic image of MV1’s iPhone 8+ phone. During his review, Det. Ellis reviewed the Snapchat application for MV1 and “K t” is listed as a contact. Det. Ellis also reviewed numerous images in which MV1 is in sexually suggestive poses and images in which MV1’s bare vagina and breasts are depicted, including images that also depict MV1’s face. I have since reviewed the forensic image of MV1’s iPhone 8+ and observed the images referenced by Det. Ellis. I observed a total of fifty-seven

(57) files, which include both still images and "live" images, at least fifty- two (52) of which are sexually explicit.

d. On June 1, 2020, Det. Ellis interviewed MV1. The interview was audio and video recorded. I have reviewed the interview in its entirety. During the interview, MV1 advised, in substance and among other things, the following:

"K t" told her his name was "Kurt" and that he lives in Putnam County. She was the only person to use her phone to communicate with "Kurt." She communicated with "Kurt" using Whisper and Snapchat. MV1 was shown screen shots of Snapchat communication between her and "K t" and confirmed they were between her and "Kurt." She met "Kurt" on Whisper, and he contacted her first. After communicating on Whisper, she and "Kurt" began using Snapchat and the communication became sexual in nature. "Kurt" requested sexually explicit images and videos of her and even directed her on how to take the images and how to pose. Some of the images she sent to "Kurt" depicted her bare vagina, breasts and buttocks. Several of the images she sent to "Kurt" depicted her inserting objects into her vagina and manipulating her vagina with her hand, which she did at "Kurt's" direction. Det. Ellis showed MV1 sexually explicit images discovered on her iPhone 8+ and she confirmed the images/videos were of her and were sent to "Kurt." She advised she lied about her age and told "Kurt" she was 15. She told "Kurt" she lived with her parents and was in school.

e. On June 4, 2020, Det. Ellis caused a subpoena to be issued to Snapchat requesting information related to username "tacticfallout." On June 8, 2020, Snapchat provided the requested information to Det. Ellis. The information has since been provided to me and I have reviewed it in its entirety. The information provided by Snapchat lists a Snapchat id of "tacticfallout," an email address of tacticfallout@gmail.com, and a creation date of September 23, 2016.

f. On July 28, 2020, Det. Ellis caused a subpoena to be issued to Snapchat requesting, among other things, IP history for username "tacticfallout." On August 17, 2020, Snapchat provided the requested information to Det. Ellis. The information has since been provided to me and I have reviewed it in its entirety. The information provided by Snapchat revealed IP address 76.106.129.121 was recorded on two occasions in January 2019 when the user logged into the account. I have since confirmed via open source research that the service provider for IP address 76.106.129.121 is Comcast with a location of Interlachen, Florida.

g. On August 4, 2020, Det. Ellis caused a subpoena to be issued to Google requesting information related to email address tacticfallout@gmail.com. On August 8, 2020, Google provided the requested information to Det. Ellis. The information has since been provided to me and I have reviewed it in its entirety. The information provided by Google revealed the account was created on December 22, 2014, and the last three login dates were

July 28, 2020, March 3, 2020, and November 27, 2019. Google also provided IP activity revealing IP address 76.106.129.121 was recorded on March 3, 2020 and November 27, 2019 when the user logged into the account.

h. On August 7, 2020, Det. Ellis caused a subpoena to be issued to Comcast for the subscriber of IP address 76.106.129.121. On August 12, 2020, Comcast provided the requested information to Det. Ellis. The information has since been provided to me and I have reviewed it in its entirety. The information provided by Comcast revealed a subscriber name of Dwight Sheldon at an address of 230 Ofarrell Avenue, Interlachen, Florida 32148, one of the two physical addresses connected to the Subject Location, as explained below.

49. On August 13, 2020, I conducted an address search using the 230 Ofarrell Avenue address within the Florida Driver and Vehicle and Information Database (DAVID) with negative results. I then queried the name "Dwight Sheldon" and discovered Dwight Austin Sheldon lists the 232 Ofarrell Avenue address as his address since March 1999. In addition, I discovered Kurt Batucan Sheldon lists the 232 Ofarrell Avenue address as his address beginning in November 2008 and his date of birth indicates he is currently twenty-nine (29) years old, as similarly conveyed by MV1.

50. On the same day, I queried the 232 Ofarrell Avenue address via the Putnam County Property Appraiser website and discovered Dwight and Jennifer Sheldon are the owners of the property with parcel 911 addresses for both 230 and 232 Ofarrell Avenue, Interlachen, Florida 32148. I have since queried the

230 Ofarrell Avenue address via the Putnam County Property Appraiser website with negative results.

51. On the same day I requested an address verification for persons receiving mail at both 230 and 232 Ofarrell Avenue, Interlachen, Florida 32148 from U.S. Postal Inspector (USPI) Keith Hannon. On August 14, 2020, USPI Hannon told me that Dwight Sheldon currently receives mail at one box that services both addresses.

52. On August 14, 2020, I asked Putnam County Sheriff's Office (PCSO) Det. Gentry to research the Subject Location and anyone associated with the Subject Location. Det. Gentry informed me her research revealed that Kurt Sheldon, among other Sheldon family members, resides at the Subject Location. In addition, Det. Gentry informed me of a 2014 report involving Kurt Sheldon at the Subject Location. Det. Gentry subsequently provided me with the report, and I have reviewed it in its entirety. This report indicated Kurt Sheldon provided 232 Ofarrell Avenue, Interlachen, Florida 32148 as his home address.

53. On August 26, 2020, I spoke with MV1's mother via telephone and inquired about a few additional details. MV1, through her mother, advised the following:

She is 99% sure she told "Kurt" she was 15 prior to sending any sexual images to him. She advised her Whisper profile age was 15-17.

54. During the course of this investigation, I learned of a prior

investigation conducted by SJSO Det. Greene involving the Sheldon name and the Subject Location. Based on my communication with Det. Greene, and my review of reports and documents provided by SJSO Det. Greene, I have learned the following, among other things:

- a. In May 2016, SJSO Det. Greene began an investigation into IP address 73.192.111.22, port 40537. A computer using the IP address was observed on the BitTorrent network with multiple images of suspected child sexual abuse material (CSAM) available for sharing on multiple occasions.
- b. A review of the records by Det. Greene associated with the IP address identified 88 files available for sharing between May 24, 2016 at 9:16 PM and May 25, 2016 at 9:18 PM. During this timeframe, Det. Greene downloaded 6 complete files. There were also several partially downloaded files which were not complete but somewhat viewable. The image files that were downloaded appeared to be clips from a larger video file, possibly the incomplete video associated with this torrent.
- c. Between May 26, 2016 at 5:09 PM and May 27, 2016, Det. Greene observed another torrent associated with the same IP address which noted that 353 files were available for sharing. During this timeframe, Det. Greene downloaded 3 complete files.
- d. Det. Greene subsequently caused a state subpoena to be issued to Comcast on July 11, 2016, requesting account holder/subscriber

information for the dates and times mentioned above for IP address 73.192.111.22, port 40537. On July 12, 2016, Comcast provided the requested information advising IP address 73.192.11.22:40537 was assigned to Dwight Sheldon at 230 Ofarrell Avenue, Interlachen, FL 32148.

55. On August 17, 2020, I retrieved the images and documentation referenced above. On August 25, 2020, I along with Det. Ellis, reviewed the files downloaded by Det. Greene as mentioned above. My description of one of the files downloaded on May 26, 2016 is as follows: The image depicts a pre-pubescent female child lying on what appears to be a bed covered with an orange sheet. The child is wearing a small bathing suit top that covers her breasts only and is naked from that point down. The child is posed in an unnatural and sexually suggestive manor in which her legs are spread, thereby exposing her bare vagina. The same pre-pubescent child is depicted in the other two images downloaded on the same date and depicts her in the same clothing and setting, and in two separate, unnatural, and sexually suggestive poses in which her bare vagina is exposed. I have probable cause to believe this is a child due to the overall body size, lack of breast development, lack of pubic hair, child-like facial features, and overall size of the child's body. Based on my training and experience and my review of this image, I have probable cause to believe that the image constitutes child pornography, that is, a visual depiction of a minor engaged in sexually explicit conduct as set forth in 18 U.S.C. § 2256.

### CONCLUSION

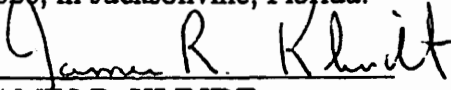
56. Based on the foregoing, I have probable cause to believe that one or more individuals has used and is using one or more computer devices, wireless telephones, and/or electronic storage media on the premises containing two residential trailers, an additional large structure, and multiple sheds located at two physical addresses of 230 and 232 Ofarrell Avenue, Interlachen, Florida 32148, more fully described in Attachment A to this affidavit to, among other things, receive, distribute, and possess child pornography. In my training and experience, I know computer devices, wireless telephones, and/or electronic storage media, can be stored in a variety of large and small locations anywhere on a premises, to include structures similarly observed on this premises, and further described in Attachment A. Therefore, I have probable cause to believe that one or more individuals, using the premises described above has violated 18 U.S.C. §§ 2252 and/or 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 device and/or other electronic storage

media containing images and/or video depicting child pornography, and the items more fully described in Attachment B to this affidavit (which is incorporated by reference herein), will be located on this premises.



Benjamin J. Nuecke, Special Agent  
Homeland Security Investigations

Sworn and subscribed to via telephonic means on this 2nd day of September, 2020, in Jacksonville, Florida:



JAMES R. KLINDT  
United States Magistrate Judge

## ATTACHMENT A

### **Premises to be Searched**

The premises to be searched is the lot on a dirt road at the corner of Ofarrell Avenue and Fowler Street, including the physical addresses of both 230 and 232 Ofarrell Avenue, Interlachen, FL 32148. A grey chain link fence, approximately 6 feet in height, appears to surround part of the premises. A "No Trespassing" sign is affixed to the gate part of the fence on Ofarrell Avenue. A white mailbox on a wooden post with black "232" stickers is situated directly across from the premises on Ofarrell Avenue. There appears to be two trailers on the property, as well as an additional large structure and multiple sheds.



JRK

**ATTACHMENT B**

**DESCRIPTION OF ITEMS TO BE SEARCHED AND SEIZED**

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, wireless telephones, “smart” phones, electronic tablets, 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 peer to peer software, that may be or are used to: visually depict child pornography (any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)) 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 described above, 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, 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).

17. Any documents, records, programs or applications relating to the existence of wiping, data elimination, and/or counter-forensic programs (and associated data) that are designed to delete data from the subject computers and computer media.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☐ Original☐ Duplicate Original

## 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)The premises located at 230/232 Ofarrell Avenue,  
Interlachen, FL 32148, as further described in  
Attachment A

Case No. 3:20-mj-1290-JRK

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Middle District of Florida  
(identify the person or describe the property to be searched and give its location):

the premises located at 230/232 Ofarrell Avenue, Interlachen, FL 32148, as further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):  
See Attachment B.YOU ARE COMMANDED to execute this warrant on or before 9-11-2020 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to James R. Klindt  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for        days (not to exceed 30) ☐ until, the facts justifying, the later specific date of       Date and time issued: 9-2-2020 at 2:03 PMCity and state: Jacksonville, FloridaJames R. Klindt  
Judge's signature  
James R. Klindt, United States Magistrate Judge  
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

**Return**

Case No.:

3:20-mj- 1290 - JRK

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

**Certification:**

I declare under penalty of perjury that this inventory is correct and was returned electronically along with the warrant to the designated judge pursuant to Fed. R. Crim. P. 4.1 and 41(f)(1)(D).

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## ATTACHMENT A

### **Premises to be Searched**

The premises to be searched is the lot on a dirt road at the corner of Ofarrell Avenue and Fowler Street, including the physical addresses of both 230 and 232 Ofarrell Avenue, Interlachen, FL 32148. A grey chain link fence, approximately 6 feet in height, appears to surround part of the premises. A "No Trespassing" sign is affixed to the gate part of the fence on Ofarrell Avenue. A white mailbox on a wooden post with black "232" stickers is situated directly across from the premises on Ofarrell Avenue. There appears to be two trailers on the property, as well as an additional large structure and multiple sheds.



JRK

**ATTACHMENT B**

**DESCRIPTION OF ITEMS TO BE SEARCHED AND SEIZED**

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, wireless telephones, "smart" phones, electronic tablets, 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 peer to peer software, that may be or are used to: visually depict child pornography (any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)) 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 described above, 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, 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).

17. Any documents, records, programs or applications relating to the existence of wiping, data elimination, and/or counter-forensic programs (and associated data) that are designed to delete data from the subject computers and computer media.

JRK