

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 6:19-cr-1-Orl-40LRH

RONALD HILL,

Defendant.

_____ /

DEFENDANT’S MOTION TO SUPPRESS EVIDENCE

Defendant, Ronald Hill, by and through his undersigned attorney, moves this Honorable Court, pursuant to the Fourth Amendment of the United States Constitution and Fed. R. Crim. P. 12(b)(3)(C), to suppress all documents, files, records, and data, from all computers, electronic devices,¹ storage media, and cell phones, seized subject to the warrant issued on December 4, 2018 and executed on December 6, 2018.² The Fourth Amendment requires that searches conducted pursuant to a warrant not exceed its strict bounds. The warrant in this matter authorized the search of the defendant’s home, and seizure of his computers and electronic devices, but did not authorize the subsequent search of those devices. In support of this motion, the Defendant submits this memorandum of law.

¹ “Electronic devices”, in this memo, is employed as a catch-all designation which includes cellular phones – both “smart” and those without data/internet capacities – gaming console and devices, desktop computers and laptops, and all computer peripheral devices.

² Because the basis for suppression deals with the *execution* of the warrant, a *Leon* “Good Faith” analysis is unnecessary. *Leon* dealt with an invalid warrant relied on in good faith by the executing officers and its analysis in large measure relied on an assumption “that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant.” *United States v. Leon*, 468 U.S. 897, 918 n. 19 (1984); *see also* 1 W. LaFare, *Search and Seizure*, § 1.3(f) (5th ed. Updated Oct. 2018) (“Fourth Amendment violations relating to execution of the warrant are unaffected by *Leon*, as is indicated by the majority’s caution that its discussion ‘assumes, of course, that the officers properly executed the warrant and searched only those places for those objects that it was reasonable to believe were covered by the warrant.’”).

CHARGES

The Defendant, Ronald Hill, was charged by Indictment, filed on January 3, 2019, with one count of distribution of child pornography in violation of 18 U.S.C. § 2252A(a)(2), and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). *See* Indictment at Doc. 10.

FACTUAL BACKGROUND

On or about December 4, 2018, Special Agent (SA) Kevin Kaufman, with the Federal Bureau of Investigation (FBI) made an Application for a Search Warrant, to search the home of Ronald Hill located at 131 N. Aberdeen Circle, Sanford, Florida 32773 (the application). Exhibit A. In addition to SA Kaufman's Affidavit in Support of Search Warrant, SA Kaufman appended "Attachment A," describing the place to be searched, that is, Mr. Hill's house. Exhibit A, Attachment A. Additionally, SA Kaufman appended "Attachment B," the "Description of Items to be Searched for and Seized," which described and defined the evidence sought for seizure. Exhibit A, Attachment B.

At 11:19 am on December 4, 2018, the Honorable Karla R. Spaulding, United States Magistrate Judge, issued a Search and Seizure Warrant (the warrant). Exhibit B. The face of the warrant, where it identified "the person or [...] property to be searched" states "131 N. Aberdeen Circle, Sanford, Florida 32773," as described in Attachment A to the warrant, which is consistent with Attachment A to the application. It does not request to search any computers, devices, or storage media. Where the warrant finds that probable cause was established "to search and seize," it references "the person or property described above," referencing Attachment A; that is, Mr. Hill's home address. The warrant also provides "that such search will reveal (*identify the person or describe the property to be seized*): See Attachment B," which lists the contraband and

instrumentalities and is consistent with Attachment B to the application. There was no judicial determination of probable cause to authorize the subsequent search of the electronic devices seized.

On December 6, 2018, SA Kaufman, along with a team of FBI agents and local law enforcement officers executed the warrant at Mr. Hill's residence. Doc. 1 at 4. The search resulted in the seizure of a WD Hard Drive S/N: WCC2EP467187; a Samsung camera with SD card; a Toshiba laptop S/N: YF127422C; and a Z modo DVR. Govt. Bates 0093. None of the agents sought Mr. Hill's consent to search any of the electronic devices found in his home. Nevertheless, during the search, Special Agent Alexis Brignoni searched the electronic data contents of Mr. Hill's seized laptop computer. Doc. 1 at 6. No new warrant was sought prior to this search.

ARGUMENT

Citizens have a heightened privacy interest in electronic devices that contain 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time. *United States v. Lichtenberger*, 786 F.3d. at 478, 488 (6th Cir. 2018) (citing *Riley v. California*, 134 S. Ct. 2473, 2489). This includes computers. *See, e.g., Id.; United States v. Thomas*, 818 F.3d 1230,1242 (11th Cir. 2016). This heightened privacy interest informs Fourth Amendment analysis. *E.g., Riley* (requiring a warrant for a search incident to arrest); *United States v. Sparks*, 806 F.3d 1323, 1336 (11th Cir. 2015) (finding that a private search of a cell phone "did not expose every part of the information contained in the cell phone."); *Lichtenberger* at 488 ("under *Riley*, the nature of the electronic device greatly increases the potential privacy interests at stake, adding weight to one side of the scale while the [government's interests in conducting the search] remains the same.").

A search and seizure by law enforcement officers infringe on two separate and distinct interests: a search invades a person's privacy whereas a seizure invades a person's possessory

interests in his person or property. *Horton v. California*, 496 U.S. 128, 133 (1990). In *Riley*, police had probable cause to arrest (seize) and search defendant to protect themselves and then search for and seize any personal property found on the defendant pursuant to the search incident to arrest doctrine. 134 S. Ct. at 2483 (citing *Chimel v. California*, 395 U.S. 752, 762-763 (1969)). As it relates specifically to electronic devices, the police in *Riley* were authorized to seize defendant's cell phone upon his arrest, not for officer safety, but to prevent the destruction of evidence. But it was not the physical cell phone itself that would contain evidence of an offense, but rather the data or information stored inside of it. Despite authority to seize the phone believing it contained evidence, however, the police still needed a warrant to search it. The same was true with the seizure of Mr. Hill's laptop. *Cf. United States v. Fulton*, 914 F.3d 390, 396 (5th Cir. 2019) (“[I]f a search warrant specifically names a cellphone only as one of the objects to be seized, absent exigent circumstances a search warrant will thereafter be required to authorize a search of that cellphone.”).

The Fourth Amendment expressly guarantees, “no Warrants shall issue, but upon probable cause....” In the instant case, the warrant clearly stated that probable cause was established to support the search and seizure of the “person or property described above.” Exhibit B. The only “property described above” was Mr. Hill's home (described in more detail in Attachment A to the warrant). The probable cause finding could also arguably extend to supporting a seizure of all electronic devices and data found within the home (as described in Attachment B to the warrant). But judicial authorization to search Mr. Hill's home and seize all electronic devices and data within the home was not authorization to then perform a search of the data contents of the electronic devices seized. In fact, Rule 41 of Federal Rules of Criminal Procedure, under the subsection “Contents of the Warrant,” allows for later review of seized media or electronically stored

information so long as it is “consistent with the warrant.” Fed. R. Crim. P. 41(e)(2)(B). Nothing in the contents of the warrant in the instant case provided for a subsequent search through the data of the electronic devices at issue, and nothing in Rule 41 dispenses with the probable cause requirement.

Furthermore, a legitimate basis for law enforcement to override an individual’s privacy interests in an electronic device does not extend to each piece of data in that device. *See, e.g., Sparks*, 806 F.3d at 1336 (“While...private search of the cell phone might have removed certain information from the Fourth Amendment’s protections, it did not expose every part of the information contained in the cell phone.”). Even if SA Kaufman intended such a broad search in his application, “[t]he mere fact that the Magistrate issued a warrant does not necessarily establish that he agreed that the scope of the search should be as broad as the affiant’s request.” *Groh v. Ramirez*, 540 U.S. 551, 561 (2004).

The warrant in the instant case only authorized a seizure of electronic devices and specific data within those devices (listed in Attachment B to the warrant). Because it is simply not possible to seize data within an electronic device without seizing the device that stores said data, the seizure of all electronic devices already satisfied law enforcement’s interests by overriding Mr. Hill’s possessory interests in those items. Especially since *Riley*, however, in order for the FBI to also override Mr. Hill’s privacy interests in those devices, another search warrant was needed. As the Supreme Court in *Riley*, the Eleventh Circuit in *Sparks*, and the Fifth Circuit in *Fulton* have recognized, authorization to only seize electronic devices that can contain an immense amount of data is not authorization to then search the devices without another warrant. *See also, United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009) (holding that a motion to suppress should have been granted where agents had an unreasonable delay in obtaining a search warrant after seizing

computers based on defendant admitting it contained child pornography). Moreover, “the Fourth Amendment confines an officer executing a search warrant strictly within the bounds set by the warrant.” *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 395 n. 7 (1971).

The lack of a probable cause finding to search all of the seized electronic devices resulted in a violation of Mr. Hill’s Fourth Amendment rights. Because the FBI agents were not authorized to search the electronic devices seized from Mr. Hill’s home without another search warrant, all evidence obtained as a result of that unlawful search must be suppressed. There can be no doubt that suppression of evidence in this case will deter law enforcement agents from repeating this violation in future cases. The FBI’s conduct in this case was “sufficiently deliberate” that exclusion of evidence “can meaningfully deter it.” *Herring v. United States*, 555 U.S. 135, 144 (2009). After all, “[i]t is incumbent on the officer executing a search warrant to ensure the search is lawfully authorized and lawfully conducted.” *Groh*, 540 U.S. at 563.

OBJECTION BY THE GOVERNMENT

The undersigned counsel has conferred with the Assistant United States Attorney, Ilianys Rivera Miranda, and the government objects to the instant motion.

REQUEST FOR EVIDENTIARY HEARING

Mr. Hill submits that the exhibits attached to the instant motion, the application and the warrant, provide for a sufficient basis for this Court to derive the facts necessary on which to render its ruling, without the necessity of any witness testimony. To the extent that this Court may have any unanswered inquiries into the facts and circumstances pertaining to the warrant at issue, Mr.

Hill respectfully submits that an evidentiary hearing would then be required. *United States v. Sneed*, 732 F.2d 886 (11th Cir. 1984).

CONCLUSION

Wherefore, the Defendant, Mr. Hill respectfully moves this Court to suppress any evidence derived from the unlawful search of his computers, electronic devices, and storage media.

Respectfully submitted,

Donna L. Elm
Federal Defender

/s/ Joshua R. Lukman
Joshua R. Lukman
Assistant Federal Defender
Florida Bar No. 0088213
201 S. Orange Avenue, Suite 300
Orlando, Florida 32801
Telephone: 407-648-6338
Facsimile: 407-648-6095
E-Mail: joshua_lukman@fd.org

CERTIFICATE OF SERVICE

I Hereby Certify that undersigned electronically filed the foregoing *Defendant's Motion to Suppress Evidence* with the Clerk of Court (CM/ECF) by using the CM/ECF system which will send a notice of electronic filing to the following: Ilianys Rivera Miranda, Assistant United States Attorney, this the 24th day of May, 2019.

/s/ Joshua R. Lukman
Joshua R. Lukman

EXHIBIT A

APPLCIATION FOR A SEARCH WARRANT

(Bates # 0102 – 0135)

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)

Property located at
131 N. Aberdeen Circle, Sanford, Florida 32773
See Attachment A.

Case No. 6:18-mj-1766

APPLICATION FOR A SEARCH WARRANT

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

131 N. Aberdeen Circle, Sanford, Florida 32773. See 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.

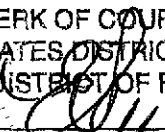
The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- 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
18 U.S.C. §§ 2252A(a)(2) and
2252A(a)(5)(B)

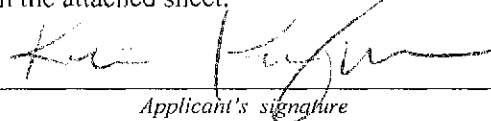
Offense Description
Possession and distribution of child pornography

THE FOREGOING TO BE A TRUE
AND CORRECT COPY OF THE ORIGINAL
CLERK OF COURT
UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
BY: 
DEPUTY CLERK

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

Kevin Kaufman, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/4/2018



Judge's signature

KARLA R. SPAULDING, United States Magistrate Judge

Printed name and title

City and state: Orlando, Florida

STATE OF FLORIDA

CASE NO. 6:18-mj-1766

COUNTY OF ORANGE

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kevin Kaufman, being duly sworn, do hereby depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 131 N. Aberdeen Circle, Sanford, Florida 32773 (hereinafter the "PREMISES," which is further described in Attachment A), for the things described in Attachment B.

2. I have been a Special Agent (SA) with the Federal Bureau of Investigation (FBI) for the past 14 years. I am currently assigned to the FBI Violent Crimes Against Children Task Force.

3. I have received specialized training concerning investigations of sex crimes, child exploitation, child pornography, and computer crimes. I have also investigated and assisted in the investigation of matters involving the possession, receipt, distribution, and production of child pornography. During the course of my training and investigations, I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a SA who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A(a).

4. I have participated in various training courses concerning the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography.

Additionally, I have participated in the execution of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information.

5. I make this affidavit based on my experience and background as a law enforcement officer, including my experience with the FBI; my personal participation in the investigation; and information provided by SA Michelle Langer, and other law enforcement officers and agency personnel. As set forth in more detail below, I have probable cause to believe that a crime has taken place, that is, the knowing possession and distribution of child pornography in interstate commerce, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B). Furthermore, I have probable cause to believe that the PREMISES to be searched contains instrumentalities, contraband, and evidence of these crimes, as set forth in Attachment B.

6. I am requesting authority to search the entire PREMISES—including the curtilage, residential dwelling(s), and any computer, computer media, or electronic storage devices located therein, where the items specified in Attachment B may be found. I also request to seize all items listed in Attachment B as instrumentalities, contraband, and evidence of criminal activity.

7. Because I am submitting this affidavit for the limited purpose of seeking a search warrant, I have not set forth each and every fact that I learned during the course of this investigation.

STATUTORY AUTHORITY

8. It is a violation of 18 U.S.C. § 2252A(a)(2) to knowingly distribute child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate commerce, or in or affecting interstate commerce. It is a violation of 18 U.S.C. § 2252A(a)(5) to knowingly possess child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate commerce, or in or affecting interstate commerce.

DEFINITIONS

9. The following definitions apply to this affidavit and to Attachment B:

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, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. “Child Pornography,” as used herein, is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involves 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. § 2256(8).

c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *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 “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]” *See* 18 U.S.C. § 1030(e)(1)

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, flash memory cards, thumb drives 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 that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

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

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. 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, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as digital cameras, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, laptop computers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

10. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was primarily produced using cameras and film (either still photography or movies). Development and reproduction of the images often required darkroom facilities and a significant amount of skill, and there were definable costs involved with the production of pornographic images. Distribution of child pornography on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a

combination of personal contacts, mailings, and telephone calls. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

11. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. 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.

12. 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 (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

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

14. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as, Dropbox, Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail 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.

15. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (e.g., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files). Digital information can also be retained unintentionally. Thus 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). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, was using Internet Portals, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

PEER TO PEER (P2P) FILE-SHARING

16. Based on my training and experience, I have learned that computer users can choose to install publicly available software that facilitates the sharing of files. Millions of computer users throughout the world use peer-to-peer (P2P) file-sharing networks to share files containing music, graphics, movies, programs, text and the like. These networks have also become a popular way to download and distribute child pornography.

17. The Bittorrent network is one such publicly available P2P file-sharing network. Most computers that are part of this network are referred to as “peers.” A peer can simultaneously provide files to peers while downloading files from other peers. The software can balance the network load and recover from network failures by accepting pieces of a particular file from different users and then reassembling the file on the local computer. This process is accomplished by the use of hash values, which is described later in the affidavit.

18. The Bittorrent network can be accessed by peer computers via many different Bittorrent network clients (software), including the Bittorrent client, uTorrent client, and Vuze client, among others. These clients are publicly available and can usually be downloaded for free from the Internet. In normal P2P operations, as users download files or pieces of files from other peers on the Bittorrent network, other peers on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, he or she can also continue to share

the file with individuals on the Bittorrent network who are attempting to download all pieces of the file or files. A person who has all the pieces of a particular file is termed a “seeder.”

19. Files or sets of files are shared on the Bittorrent network through the use of “torrents.” A torrent is typically a small file that *describes* the file(s) to be shared. It is important to note that torrent files do not contain the actual file(s) to be shared. Instead, torrent files contain information about the file(s) to be shared that is needed to accomplish a download. Examples of this information are the name(s) of the file(s) being referenced in the torrent, the number of pieces that make up the torrent, and the “info hash” of the torrent.

20. The “info hash” is a Secure Hash Algorithm, commonly abbreviated as SHA-1, which describes the data of the file(s) referenced in the torrent. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital “fingerprint” that consists of a unique series of letters and numbers. The United States has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA hash functions, and it is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA-1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA-1 signature are identical copies of the same file, regardless of their file names.

This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The “info hash” of each torrent uniquely identifies the torrent file on the Bittorrent network.

21. 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 that have recently reported they are sharing the file(s) referenced in the torrent file. A tracker is only a pointer to peers on the network who may be sharing part or all of the file(s) referenced in the torrent. Trackers do not actually have the file(s) but are used to facilitate the finding of other peers 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 that have file(s) being shared from a particular torrent file. There are many publicly available servers on the Internet that provide Bittorrent tracker services.

22. The term “pieces” as used above refers to how many data sets are needed to complete the total download of a given torrent. The number of pieces is determined by a Bittorrent client when the torrent is created. A torrent may have one piece, or it may have thousands of pieces. A torrent is broken up into pieces as it speeds up the ability of the network to deliver the contents of the torrent from multiple users on the network. When more pieces are available, a user can obtain all the contents of a torrent file more quickly.

23. In order to locate torrent files of interest and download the files that they describe, a typical user will use keyword searches on torrent-indexing websites, such as *isohhunt.com* and *piratebay.org*. Torrent-indexing websites are essentially search engines that users on the Bittorrent network use to locate torrent files that describe the files they are looking to download. Torrent-indexing websites do not host the content (files) described by torrent files; they host only the torrent files themselves. Once a torrent file is located on the website that meets a user's keyword search criteria, the user will download the torrent file to his or her computer. The Bittorrent client on the user's computer will then process that torrent file in order to either find trackers or use other means to find 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 on the Bittorrent network—not from the trackers themselves. Typically, the trackers on the network return information about remote peers that have recently reported that they have the same file(s) available for sharing (based on SHA-1 “info hash” value comparison), or parts of the same file(s), referenced in the torrent. Such information includes the remote peer's Internet Protocol (IP) addresses.

24. Internet computers identify each other by an Internet Protocol or IP address. When a computer connects to the Internet, the Internet Service Provider (ISP) providing the Internet connection assigns that computer a specific numerical identifier called an IP address. The IP address allows the computer to communicate

with the Internet. ISPs control blocks of IP addresses and only assign a given IP address to one customer at a time.

25. IP addresses are analogous to telephone numbers. To use a telephone, the phone must have an associated phone number. To access the Internet, a computer must be assigned an IP address. IP addresses can be dynamic or static. Dynamic IP addresses can and do change over time, but they can be retained by a subscriber for months or even a year or more—especially where there is a high-speed cable modem connection (like the connection in this case). Static IP addresses never change unless the customer cancels the account or requests a new static IP address.

26. I know that these IP addresses can assist law enforcement in finding a particular computer on the Internet. Once an IP address is known, a subpoena can be issued to the appropriate ISP for business records related to the subscriber assigned to that IP address at a particular time and date. The ISP will typically provide information concerning the name, address, and other identifying information of the subscriber using the particular ISP. This process has proven to be very reliable in identifying suspects using the Internet.

27. A person interested in obtaining child pornographic images or videos on the Bittorrent network can go to a torrent-indexing website and conduct a keyword search using a term such as “preteen sex” or “pthc” (pre-teen hardcore). The results of the keyword search are typically returned to the user’s computer by displaying them on the torrent-indexing website. Based on the results of the keyword search, the user would then select a torrent of interest to them to download to their computer from the

website. Typically, the Bittorrent client program will then process the torrent file, which acts like a road map in allowing the Bittorrent client to obtain the necessary information to go out on the Bittorrent network and find others peers with the files embedded in the torrent. Utilizing trackers and other Bittorrent network protocols, peers are located that have recently reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) are then downloaded directly from the computer(s) sharing the file(s).

28. Typically, once the Bittorrent network client has downloaded part of a file(s), it may immediately begin sharing the part of the file(s) it has 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 hash value of that piece which is described in the torrent file. The downloaded file(s) are then stored in an area (folder) previously designated by the user and/or the Bittorrent client on the user’s computer or designated external storage media. The downloaded file(s), including the torrent file, will remain in that location until moved or deleted by the user.

29. Law enforcement can search the Bittorrent network in order to locate individuals who are sharing previously identified child exploitation torrents in the same way that a user searches this network. By searching the Bittorrent network for these known torrents, law enforcement can quickly identify targets in a given jurisdiction that may be in possession of and/or distributing known or suspected files of child pornography. Through trackers, law enforcement receives information about

peers on the Bittorrent network who recently reported involvement in sharing digital files of known or suspected child pornography based on SHA-1 info hash value(s) of torrent(s). The torrents that law enforcement searches for are those that law enforcement previously identified as being associated with such files depicting known or suspected child pornography.

30. There are Bittorrent clients that only allow single-source downloads from a computer at a single IP address. In other words, an entire file can be downloaded only from a computer at a single IP address, as opposed to obtaining the file from multiple peers on the Bittorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the Bittorrent network.

31. During the query and/or downloading process from a suspect's Bittorrent client, certain information may be exchanged between the investigator's Bittorrent client and the suspect's Bittorrent client. This information includes: (a) the suspect client's IP address; (b) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and (c) the Bittorrent network client program and version being utilized by the suspect computer. The law enforcement Bittorrent client has the ability to log this information.

32. I have been involved in numerous P2P search warrants and have consulted with many experienced investigators who have used this method of investigation. Nearly every case was verified through the following means:

- a. Evidence of child pornography was found on the computer;
- b. If no images of child pornography were found on the computer, interviews of persons using those computers verified that child pornography had been present at one time but had since been deleted, or the computer with the child pornography had been removed from the premises. In rare cases, it was determined that the suspect accessed the customer's unsecured wireless router and thereby downloaded child pornography using his IP address. In such cases, the unsecured wireless router was an instrumentality of the crime subject to seizure in that it aided in the receipt and distribution of child pornography and potentially contained data logs.
- c. Images were moved from a computer and stored on other media.

DETAILS OF THE INVESTIGATION

33. On November 12, 2018, SA Langer—acting in an undercover capacity and using a P2P file-sharing program known as Bittorrent Roundup—downloaded multiple images and videos of child pornography from a computer using IP address 184.90.145.34. On November 12, 2018, the P2P file-sharing program determined IP address 184.90.145.34 was sharing a torrent with the info hash: 51d49fa4fafe9f2268dcac0bec1daa6c5d894575. This torrent file references 23 files, at least one of which is a file of investigative interest to child pornography investigations.

34. On November 12, 2018, between 5:53 p.m. and 5:56 p.m., SA Langer completed a single-source download from IP address 184.90.145.34. During the single-source download, SA Langer downloaded two complete files and three partially complete files. Two of the complete files I viewed are described as follows:

- **“(Pfhc)6Yo Babyj – Bedtime Rape.mpg”**: The video is approximately 1 minute 5 seconds in length. The video features a female child approximately 4-5 years old. The 4-5 year old child is naked on a bed under a bed sheet. An adult male performs oral sex on the child, digitally penetrates the child’s vagina, and masturbates until he ejaculates onto the child’s vagina.
- **“12 yo girl raped.avi”**: The video is approximately 2 minutes 1 second in length. The video features a female child approximately 11-12 years old. The child’s legs are bounded while an adult male vaginally and anally rapes the child until he ejaculates on the child’s stomach.

35. I have reviewed the complete files and incomplete files from SA Langer’s undercover session on November 12, 2018. During the review, I determined that five of the complete or partially downloaded videos contain child pornography. I viewed one of the partially complete downloads along with the two complete files downloaded and determined the files contain child pornography, as defined in 18 U.S.C. § 2256.

36. A query of the IP address 184.90.145.34 was made through the American Registry for Internet Numbers (ARIN). ARIN reported that IP address 184.90.145.34 was registered to Charter Communications, Incorporated (Charter Communications).

37. On November 15, 2018, a subpoena was served to Charter Communications regarding IP address 184.90.145.34 to obtain certain subscriber

information in effect as of November 12, 2018. Charter Communications returned the following information in response to the subpoena:

Customer Name: R.H.
Service Address: 131 N. Aberdeen Circle
Sanford, Florida 32773
(Namely, the PREMISES)
Time of Download: Active since April 26, 2018, and assigned to the PREMISES.

38. The address listed on the subscriber information was run through the Florida Driver and Vehicle Identification Database (DAVID) and showed it as the primary residence of R.H. and E.H., 131 N. Aberdeen Circle, Sanford, Florida 32773. Additionally, their son, R.H. Jr., had utilized that address as a primary residential address since May 2018. Thereafter, I conducted surveillance of the residence, during which I observed a silver Toyota Corolla bearing a Florida license plate at the PREMISES. I conducted a search of the license plate number in DAVID and determined the vehicle was registered to E.H.

**RELEVANT INFORMATION REGARDING PERSONS
INVOLVED IN THE POSSESSION AND
DISTRIBUTION OF CHILD PORNOGRAPHY**

39. Based upon my own knowledge and experience in child sexual exploitation and child pornography investigations, I know the following:

a. Persons who are involved with child pornography generally have other sexually explicit materials related to their interest in children, which may consist of photographs, motion pictures, videos, text material, computer graphics and digital

or other images for their own sexual gratification, often including child erotica, which may consist of images or text writing involving sex with minors that do not rise to the level of child pornography but nonetheless fuel their deviant sexual fantasies involving minors. I am aware that this sort of material has been admitted in trials under Fed. R. Evid. 404(b) to prove such things as the possessor's knowledge, intent, motive and identity and under Fed. R. Evid. 414 to prove the person has a sexual interest in minors.

b. 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. They do this to gain status, trust, acceptance, and support and to increase their collection of illicit images and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P chat and file-sharing programs, e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, Internet clubs, and various forms of Instant Messaging such as Yahoo Messaging.

c. Besides sexual photos of minors and child erotica, such individuals often produce and/or collect other written material on the subject of sexual activities with minors, which range from fantasy stories to medical, sociological, and psychological writings, which they save to understand and justify their illicit behavior and desires.

d. Individuals who collect child pornography often collect, read, copy or maintain names, addresses, including e-mail addresses, phone numbers, and

lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests, or have child pornography and child erotica for sale or trade. These contacts are maintained for personal referral, exchange or, sometimes, commercial profit. They may maintain these names on computer storage devices, websites or other Internet addresses, and their discovery can serve as leads to assist law enforcement in proving the instant case and in apprehending others involved in the underground trafficking of child pornography.

e. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. 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.

COMPUTER DATA

40. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on

a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. Probable cause. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a

few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

42. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to

understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to

draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to possess child pornography and to distribute child pornography over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records

of Internet discussions about the crime; and other records that indicate the nature of the offense.

43. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

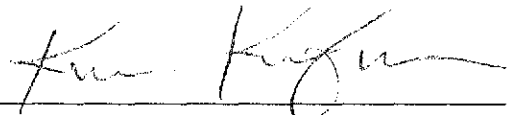
c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

44. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.


CONCLUSION

45. I submit that this affidavit sets forth probable cause for a warrant to (a) search the PREMISES described in Attachment A and (b) seize the items described in Attachment B.

Affiant further sayeth naught.


Kevin Kaufman, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 4th day of December, 2018.


KARLA R. SPAULDING
United States Magistrate Judge

ATTACHMENT A

The property located at 131 N. Aberdeen Circle, Sanford, Florida 32773 (the "PREMISES"), is within a brown brick and tan panel two-story house with a gray shingled roof. The address 131 of the residence is affixed to the right of the front door. The residence contains a two-car tan garage door with windows on the top of the garage door.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

The following items to be seized constitute instrumentalities, contraband, and evidence of violations of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B), which may be found at the PREMISES, including:

- a. Images of child pornography, as defined in 18 U.S.C. § 2256.
- b. Any record or document pertaining to the possession, receipt, and/or distribution of child pornography, as defined in 18 U.S.C. § 2256.
- c. Any record or document identifying persons transmitting, through interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.
- d. Any record or document bearing on the production, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.
- e. Any record or document 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 commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any record or document which lists names and addresses of any minor visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any record or document which shows the offer to transmit through interstate commerce any depictions of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

h. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as “child erotica” and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. “Child erotica” may also include, in this context, sex aids and/or toys.

i. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with, or about, a minor that are sexually explicit in nature, as defined in 18 U.S.C. § 2256.

j. Any documents, records, programs, or applications that identify the residents of the PREMISES.

k. Computers or storage media used as a means to commit the violations described above.

l. Any documents, records, programs or applications that identify the Internet service provided to the PREMISES.

m. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, "chat," instant messaging logs, photographs, and correspondence;

2. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the lack of such malicious software;

4. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

5. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

6. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
8. evidence of the times the COMPUTER was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
10. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
11. records of or information about Internet Protocol addresses used by the COMPUTER;
12. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
13. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications, files or materials created, modified or stored in any form, including by computer hard drives, external hard drives, thumb drives, cell-phones, smart phones, floppy disks, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage devices.

EXHIBIT B

SEARCH AND SEIZURE WARRANT

(Bates # 0095 – 0101)

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)) Property located at) 131 N. Aberdeen Circle, Sanford, Florida 32773) See Attachment A.)	Case No. 6:18-mj-1766
--	-----------------------

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search 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):

131 N. Aberdeen Circle, Sanford, Florida 32773. See 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 December 17, 2018 (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 KARLA R. SPAULDING
 (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: 12/4/2018 at 11:19

Karla R. Spaulding

 Judge's signature

City and state: Orlando, Florida

KARLA R. SPAULDING, United States Magistrate Judge

 Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.: 6:18-mj-1766	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 of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

ATTACHMENT A

The property located at 131 N. Aberdeen Circle, Sanford, Florida 32773 (the "PREMISES"), is within a brown brick and tan panel two-story house with a gray shingled roof. The address 131 of the residence is affixed to the right of the front door. The residence contains a two-car tan garage door with windows on the top of the garage door.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

The following items to be seized constitute instrumentalities, contraband, and evidence of violations of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B), which may be found at the PREMISES, including:

- a. Images of child pornography, as defined in 18 U.S.C. § 2256.
- b. Any record or document pertaining to the possession, receipt, and/or distribution of child pornography, as defined in 18 U.S.C. § 2256.
- c. Any record or document identifying persons transmitting, through interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.
- d. Any record or document bearing on the production, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.
- e. Any record or document 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 commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any record or document which lists names and addresses of any minor visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any record or document which shows the offer to transmit through interstate commerce any depictions of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

h. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as “child erotica” and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. “Child erotica” may also include, in this context, sex aids and/or toys.

i. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with, or about, a minor that are sexually explicit in nature, as defined in 18 U.S.C. § 2256.

j. Any documents, records, programs, or applications that identify the residents of the PREMISES.

k. Computers or storage media used as a means to commit the violations described above.

1. Any documents, records, programs or applications that identify the Internet service provided to the PREMISES.

m. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, "chat," instant messaging logs, photographs, and correspondence;

2. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the lack of such malicious software;

4. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

5. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

6. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
8. evidence of the times the COMPUTER was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
10. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
11. records of or information about Internet Protocol addresses used by the COMPUTER;
12. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
13. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications, files or materials created, modified or stored in any form, including by computer hard drives, external hard drives, thumb drives, cell-phones, smart phones, floppy disks, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage devices.