

FILED
1-13-2020CLERK, U.S. DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE, FLORIDA

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America)

v.)

COLUMBUS DONAVAN JEFFREY)

Case No.)

3:20-mj- 1017-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.

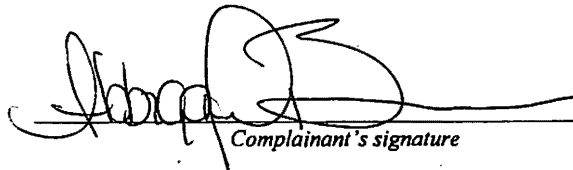
On or about the date(s) of May 3, 2019 in the county of Duval in the
Middle District of Florida, the defendant(s) violated:*Code Section**Offense Description*

18 U.S.C. § 2251(a)

Production of child pornography

This criminal complaint is based on these facts:

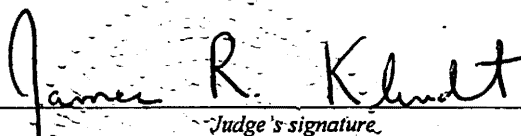
See attached affidavit.

☒ Continued on the attached sheet.
Complainant's signature

SA Abbigail Beccaccio, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 1-13-20City and state: Jacksonville, Florida
Judge's signature

United States Magistrate Judge James R. Klindt

Printed name and title

AFFIDAVIT

I, Abbigail Beccaccio, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2012. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes. Prior to this assignment, I was employed as Forensics and Technology Unit Supervisor with the Orlando Police Department for approximately 8 years. I have a Bachelor's degree in Molecular Biology & Microbiology. I have received law enforcement training from the FBI Academy at Quantico, Virginia. A substantial portion of my duties are dedicated to investigating cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate child exploitation offenses. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the solicitation of, possession, collection, production, receipt, and/or transportation of images of child pornography and the solicitation and extortion of children to produce sexually explicit images of themselves. I have been involved in searches of residences pertaining to the solicitation of, possession, collection, production, and/or transportation of child pornography through

JBK

either the execution of search warrants or through the subject providing written consent to permit a search to be conducted.

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, have been the affiant for multiple search warrants and conducted interviews of defendants and witnesses, and have served as an undercover agent in online child exploitation cases. I am a member of a local child pornography task force comprised of the FBI, U.S. Immigration and Customs Enforcement, the Florida Department of Law Enforcement, the Jacksonville Sheriff's Office, the St. Johns County Sheriff's Office, and the Clay County Sheriff's Office, 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 experienced

Special Agents and other law enforcement officers and personnel. 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 to believe that COLUMBUS DONAVAN JEFFREY has committed a violation of 18 U.S.C. § 2251(a), that is, production of child pornography.

4. I make this affidavit in support of a criminal complaint against COLUMBUS DONAVAN JEFFREY, that is, on or about May 3, 2019, in the Middle District of Florida, COLUMBUS DONAVAN JEFFREY, did employ, use, persuade, induce, entice and coerce a minor to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, and which visual depictions were produced using materials that have been mailed, shipped and transported in and affecting interstate and foreign commerce, in violation of 18 U.S.C. § 2251(a).

5. On or about October 22, 2019, I spoke with Jacksonville Sheriff's Office (JSO) Detective (Det.) A. M. Arteaga, and he provided information about an ongoing investigation of COLUMBUS DONAVAN JEFFREY for violations of Florida statutes involving child sexual exploitation. I know that Det. Arteaga is a sworn JSO Deputy Sheriff assigned to the JSO Internet

Crimes Against Children (ICAC) Unit, and is a member of the North Florida ICAC and therein conducts investigations involving internet crimes against children. The investigation resulted in the issuance of a Florida state residential search warrant, which I have reviewed and which is attached as Exhibit A, for COLUMBUS DONAVAN JEFFREY's residence located at 2154 W. 16th Street, Jacksonville, Florida, on October 3, 2019. This warrant was executed on the same day and COLUMBUS DONAVAN JEFFREY was arrested following the execution of the warrant by members of the Jacksonville Sheriff's Office in Jacksonville, Florida.

6. Det. Arteaga has provided me with documentation and evidence generated during this investigation, including the residential search warrant, arrest reports, digital device examination reports and recorded interviews. I have reviewed all of these items, and have had numerous conversations about this investigation with Det. Arteaga, both in person and by telephone. During the course of this investigation and through these sources of information, I learned, in substance and among other things, the following:

a. On August 12 and September 23, 2019, two separate and related Cyber Tip reports (C.T. 53500239 and C.T. 56041995) were received by JSO from the National Center for Missing and Exploited Children (NCMEC). I have reviewed the information contained in these Cyber Tip reports. Based on

my training and experience, I know that NCMEC receives Cyber Tips from individuals and business entities regarding the possible sexual exploitation of children. On September 18, 2019, Det. Arteaga was assigned C.T. 53500239, originating from Tumblr for investigation. Based on my training and experience, I know that Tumblr is a social media blogging and publishing network site service and can be used to upload and download images using the Internet. On September 25, 2019, Det. Arteaga was assigned C.T. 56041995, originating from Yahoo, Inc. for investigation. Yahoo, Inc., acquired Tumblr in 2013 and is now operated by Verizon Media. C.T. 53500239 was sent after Tumblr officials suspected multiple images depicting child sexual abuse material (CSAM) had been uploaded by a user using Internet Protocol (IP) address 76.245.76.84. Tumblr additionally provided the email address of the user as columbusjeffrey@gmail.com and the user name as "hideme1977."

b. In addition, I know that Exchangeable Image File Format (EXIF) data was imbedded on the images that were contained in C.T. 53500239 and reviewed by Det. Arteaga. Based on my training and experience, I know that EXIF data is metadata stored within images and it may include the original date and time that the image was taken, the camera settings such as shutter speed and focal length, the camera device make and model that the image was taken with, and the exact Global Positioning System (GPS) coordinates

(geographic location) where the image was taken. The EXIF data embedded in the images from C.T. 53500239 did not list the GPS coordinates (geographic location). The images did, however, show the date and time that the original images were taken, identified as beginning on May 3, 2019 at 10:16:59 p.m. and continuing on to May 3, 2019 at 10:28:57 p.m.¹ This date and time was within the same time frame that several other images from C.T. 53500239 were produced, one of which showed a facial image of COLUMBUS DONAVAN JEFFREY with what appears to be a minor male child. EXIF data showed the images were produced during the time frame from 10:16 p.m to 10:28 p.m. Additionally, EXIF data showed all images were said to be taken on a Samsung SM-J727P (which I know is also referred to as a J7 Perx) cellphone.

c. Det. Arteaga viewed all files provided by Tumblr in these Cyber Tips, identified as three videos and seven images. Two of these files were confirmed by Det. Arteaga to meet the definition of child pornography, pursuant to Section 847.001(3), Florida Statutes. Det. Arteaga then conducted a search of the IP address 76.245.76.84 that was provided in both C.T. 53500239 and C.T. 56041995, which revealed that it belonged to AT&T U-Verse in

¹ I have reviewed a JSO arrest and booking report dated October 3, 2019 detailing the arrest and interview of JEFFREY that stated that this time was UTC time instead of "p.m." Det. Arteaga has since informed me that this was incorrect and that the associated metadata confirms that the time is actually "p.m."

Jacksonville, Florida. On October 2, 2019, he caused a Florida state subpoena to be served on AT&T U-Verse for all available account information related to these Cyber Tips. AT&T responded by phone and later confirmed by email that the IP address resolved to a subscriber identified as COLUMBUS JEFFREY and with a service address of 2154 W. 16th Street, Jacksonville, Florida 32209. In addition, the email address (columbusjeffrey@gmail.com) associated with the Tumblr account where the child pornography files were uploaded to, matched the AT&T subscriber information.

d. On October 3, 2019, Det. Arteaga contacted COLUMBUS DONAVAN JEFFREY at his residence, located at 2154 W. 16th Street, Jacksonville, Florida, 32209, during the execution of the state search warrant. JEFFREY agreed to be interviewed by Det. Arteaga and Det. K. Vought, was advised of his constitutional rights, and agreed to speak to investigators. This interview was audio recorded, and I have reviewed this recording. During this interview, JEFFREY stated he currently had two male children living with him, A., who is 14 years old, and J., who is 12 years old. The children came to visit last summer but, due to family dynamics, have lived with him for the last year. JEFFREY had been taking care of them and takes them to school. JEFFREY confirmed that he was the subscriber for the AT&T Internet account active at his residence. He stated that the Internet at his home is password protected and

secure, however friends and family had the password. JEFFREY has chastised the boys for giving out the Internet password and has changed the password as recently as two weeks ago. JEFFREY stated that he owned a LG cellphone with service through Boost Mobile. JEFFREY has had telephone number 941-527-7441 since 2009-2010. JEFFREY had multiple social media accounts including Facebook, Instagram, Twitter, Snapchat, Grindr, Wickr and Hornet. JEFFREY used the email address columbusjeffrey@gmail.com for most of his accounts and stated he wasn't electronically inclined. His Snapchat username was "Columbus 1977" and he denied having any other accounts. JEFFREY did not freely let people use his phone, however, both boys had access to his phone once he (JEFFREY) entered the swipe code. JEFFREY let the boys use his phone because they didn't have service to call their families on their devices. JEFFREY did remember having access to Google photos, which he could access from different devices using the email account columbusjeffrey@gmail.com. Det. Arteaga then advised JEFFREY that he wanted to speak with him (JEFFREY) specifically about child pornography and other child abusive material. JEFFREY stated he used the username "hideme1977" on the application "Adam4Adam" and could have used it (the user name) for a Tumblr account. JEFFREY then stated he has a serious bloodborne disease and his medication sometimes made it difficult to remember

things. JEFFREY stated that the silver LG phone that was located in his bedroom was his primary phone. JEFFREY previously used a Samsung J7 cellphone, however he traded it in a few months ago for his current LG cellphone. JEFFREY viewed legal adult pornography and has come across child pornography while online. When he accidentally viewed child pornography, he said he called the police and had them wipe his computer. JEFFREY considered child pornography to be anyone under the age of eighteen depicted in a sexual way. JEFFREY has used his photo gallery and the site "Mega" to exchange images with other users over the Internet. Det. Arteaga told JEFFREY that he had reviewed chat communications between two users on Tumblr, "hideme1977" and "ecruzjr91," requesting "trades" which began in May 2019, including a "selfie" of JEFFREY with a boy. JEFFREY did not recall the specific conversation but identified the photo of himself and the depicted 12-year-old boy (who JEFFREY identified as M. and Det. Arteaga later confirmed was M.) on a sofa in his house. I know from conversations and image review with Det. Arteaga, this was the same facial image of JEFFREY and M. on the couch that was provided to Det. Arteaga by NCMEC in Cyber Tip 53500239. JEFFREY denied having any sexual relations with M.

e. Later on October 3, 2019, Det. Arteaga was able to identify the minor victim in the produced images as a child to whom COLUMBUS

DONAVAN JEFFREY had access. During the recorded interview, JEFFREY told Det. Arteaga the identity of M. and identified himself and M. in a "selfie" style photo that Det. Arteaga showed him during his interview. Det. Vought then located and conducted an interview of 12-year-old M.,² who advised that he spends several days a week at JEFFREY's house where JEFFREY takes care of him (M.) while his mother goes to work. During M.'s interview, M. disclosed to Det. Vought that JEFFREY had some sort of sexual contact with him on three separate occasions. M. remembered the first time that this happened, JEFFREY took a facial picture of the two of them together on the couch. During that same incident, M. stated that JEFFREY used his erect penis to penetrate M.'s anus. M. remembered that JEFFREY took pictures of this incident. M. also disclosed a second occasion where JEFFREY received oral sex from him (M.), and JEFFREY took a picture of the incident.³ M. then disclosed a third incident where JEFFREY again anally penetrated him with JEFFREY's erect penis. M. did not recall if pictures were taken during the third

² I have confirmed that M. has a date of birth of June XX, 2007.

³ A photograph matching this description was located on JEFFREY's LG phone as described below.

incident or exact dates, however M. did state that the last incident occurred approximately one month ago.⁴

f. During the execution of the search warrant, JSO located JEFFREY's LG G6 cellphone and conducted an on-site forensic review of this device. This revealed pictures of JEFFREY with a young boy identified as M. One of the photos was the same facial image of JEFFREY and M. on the couch that was provided to Det. Arteaga by NCMEC in Cyber Tip 53500239. Det. Arteaga has advised me that the sofa which was visible in the background of this photo appeared to match the sofa located in JEFFREY's house. The Cyber Tip also contained several pictures that were consistent with, based on M.'s physical appearance and statements made by M. during his interview with JSO Det. Vought, two photos taken from slightly different angles but depicting an erect penis penetrating an anus. There was a third image in the Cyber Tip that

⁴ Following his interview with Det. Vought, M. was taken to the Child Protective Services office in Jacksonville for sexually transmitted disease (STD) testing. M. was not interviewed at this time and only underwent testing. I know from conversations with Det. Arteaga and review of an email from Child Protective Investigator (CPI) Jasmine Farara, that M. later recanted his statements about being sexually abused by JEFFREY. On October 4, 2019, during a non-recorded interview by the Department of Children and Family Services (DCFS) CPI Farara, M. claimed that JEFFREY has never touched him in a sexual manner and additionally stated that he has never been left alone with JEFFREY, although the photographs produced on May 3, 2019 and described herein are consistent with the information provided by M. during his initial interview with Det. Vought set forth above.

was consistent based on M.'s physical appearance and statements by M., depicting an erect penis penetrating an anus. Det. Arteaga has advised me that the carpet that was visible in the background of this photo appeared to match the carpet that Det. Arteaga observed during his execution of the search warrant that was located in JEFFREY's house. A fourth image was located on JEFFREY's LG cellphone and depicted who I believe to be M. performing oral sex on an adult penis as the appearance of the child matches the appearance of M. in the selfie photograph identified by JEFFREY as M. In the photograph, M.'s face can clearly be seen and matches the appearance of M. in the selfie, which I have reviewed. This photo appears to be a "screenshot" as it depicts information along the top such as, outside temperature 83°, battery life 44%, mail, signal strength and a display time of 5:31 PM. A photograph matching this description was located on JEFFREY's LG phone during a forensic review of the device conducted later.

g. On October 3, 2019, Det. Arteaga and other JSO officers placed COLUMBUS DONAVAN JEFFREY under arrest charging him with three (3) counts of Sexual Battery, four (4) counts Produce/Promote Performance which includes Sexual Performance by a Child Under 18, four (4) counts of Sexual Performance by a Child - Possession of Child Pornography, and one (1) count Sexual Intercourse Without Disclosure of HIV, in violation

of Florida Statutes, Sections 794.011(8)(B), 827.071(3), 827.071(5) and 384.24(2) respectively.

7. On December 30, 2019, I, along with Det. Arteaga, viewed several of the produced images contained in Cyber Tip 53500239. The images were produced in a series-type fashion, all within twelve minutes of each other, and they depict a pubescent male child. These images were reported by Tumblr to NCMEC and uploaded via IP address 76.245.76.84 by username "hideme1977" to Tumblr using the Internet. Tumblr flagged the account and provided all posts from the user which took place during the period from April 10, 2019 through May 11, 2019. The Cyber Tip does not attribute a specific date/time to the reported image posts. User "hideme1977" had a verified email address, columbusjeffrey@gmail.com, associated with the creation of the Tumblr account on March 29, 2015. Four of the images are described below:

a. Creation date and time: May 3, 2019 at 10:16:59 PM

Description: The color image depicts a pubescent Caucasian male child, who has been identified by law enforcement and I have probable cause, as set forth above, to believe is M., with spread buttock cheeks. An adult penis is pressed between the child's buttocks against his anus. The adult male is not wearing a condom. The image appears to be taken from the viewpoint of the adult looking down at the child. Based on my training and experience, having

JAK

viewed thousands of images and videos depicting child pornography and together with the information set forth herein, I believe that the image depicts a minor engaged in sexually explicit conduct, that is, genital-genital sexual intercourse, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

b. Creation date and time: May 3, 2019 at 10:17:37 PM

Description: The color image depicts a pubescent Caucasian male child, who has been identified by law enforcement and I have probable cause, as set forth above, to believe is M., with spread buttock cheeks. An adult male penis is pressed between the child's buttocks against his anus. The adult male is not wearing a condom. The image appears to be taken from the viewpoint of the adult looking down at the child. This image is taken slightly further back than the preceding image and depicts more of the adult male's penis. Based on my training and experience, having viewed thousands of images and videos depicting child pornography and together with the information set forth herein, I believe that the image depicts a minor engaged in sexually explicit conduct, that is, genital-genital sexual intercourse, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

c. Creation date and time: May 3, 2019 at 10:19:12 PM

Description: The color image depicts a pubescent Caucasian male child, who has been identified by law enforcement and I have probable cause, as set forth above, to believe is M., on his knees on the ground. An adult male is straddling the child with his penis inserted in the child's spread buttocks. The adult male is not wearing a condom and the image appears slightly blurry. The image appears to be taken from the viewpoint of the adult looking down at the child while on his knees. Carpet can be seen on the ground that Det. Arteaga has told me is consistent with that found in JEFFREY's residence. Based on my training and experience, having viewed thousands of images and videos depicting child pornography and together with the information set forth herein, I believe that the image depicts a minor engaged in sexually explicit conduct, that is, genital-genital sexual intercourse, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

d. Creation date and time: May 3, 2019 at 10:28:57 PM

Description: The color image depicts a pubescent Caucasian male child, who has been identified by law enforcement and I have probable cause, as set forth above, to believe is M., and an adult sitting on a sofa taken as a "selfie." Neither are wearing a shirt and the child's mouth is partially open with his tongue pushed to the corner. The child's eyes are partially open and he appears

drowsy. Further, the forensic review of this file indicates that this image was produced within a twelve minute timeframe from the images described in paragraph 7.a, 7.b, and 7.c respectively. I recognize the adult male depicted in the image as COLUMBUS DONAVAN JEFFREY from my review of his photograph from the Florida Driver and Vehicle Identification Database. Further, Det. Arteaga confirmed the adult male pictured is COLUMBUS DONAVAN JEFFREY with whom he had contact on October 3, 2019. Det. Vought has advised that he has viewed this photo and that the child depicted is M.

8. Det. Arteaga provided me with a JSO Digital Device Examination Report, dated October 25, 2019, completed at his request by JSO Det. B. A. Bolton, which I have reviewed, and I learned, among other things, the following:

a. During the execution of the search warrant at JEFFREY's residence on October 3, 2019, a LG G6 (LG-LS993) cellular phone was located in JEFFREY's bedroom.

b. During an on-site review of this device, Det. Bolton observed multiple child notable pictures in a Dropbox folder titled "ped." One of these pictures appeared to visually match a photograph reported in the NCMEC Cyber Tip depicting JEFFREY and M. Also located within this folder

were multiple images depicting M., at least one of which depicted M. being sexually abused. This photo depicts M. performing oral sex on an adult penis. This image appears to be a "screenshot" as it depicts information along the top such as, outside temperature 83°, battery life 44%, mail, signal strength and a display time of 5:31 PM.

c. Further review of JEFFREY's LG G6 cellular phone depicted M. being sexually abused while lying on a bed. The sheets and comforter in these photos appeared to match the sheets and comforter in photos taken by JSO, which I have reviewed, in JEFFREY's bedroom during the execution of the search warrant.


d. Also located on the LG G6 cellular phone were chat conversations with an individual using the mobile application Telegram. The two parties were only identified by their assigned Telegram user ID numbers. As the parties attempted to geo-locate each other, the Telegram user with the ID 709119898 provided an approximate street address near the residence of JEFFREY and also provided the same phone number that was reported in the Cyber Tips and linked to the LG G6. During this conversation, Telegram user 709119898 indicated, among other things, that the user had regular access to multiple male children and periodic access to a 4-year-old male child. Throughout the Telegram chat, several points were observed where it appeared

that the users exchanged child notable files. These files could not be recovered within the chat thread itself, however, multiple child notable files were located in the directory “\media\0\Telegram\Telegram Images” with creation dates on July 28, 2019, the same day this conversation took place. Most of the files had creation dates within seconds of an incoming or outgoing message. Furthermore, the context of the conversation surrounding these files coincided with the content of the file. No other Telegram chats were located on the LG G6 that took place outside this date. One image 107737573_1721.jpg, located in “\media\0\Telegram\Telegram Images” lists a creation date specifically of 7/28/2019 9:34:00 PM and appears to correspond to a sent image in the Telegram chat sent on 7/28/2019 9:34:01 PM. This image depicted who I believe to be M. performing oral sex on an adult penis as the appearance of the child matches the appearance of M. in the selfie photograph identified by JEFFREY as M. In the photograph, M.’s face can clearly be seen and matches the appearance of M. in the selfie, which I have reviewed.

9. On December 31, 2019, I conducted open source research on multiple sites and learned as of 2019, Samsung has mobile phone manufacturing factories in six locations throughout the world, including facilities located in Vietnam, China, India, Brazil, Indonesia, and South Korea. Conversely, Samsung does not have any cell phone manufacturing facilities located within

the United States. Therefore, I have probable cause to believe that the Samsung SM-J727P cellphone, which I know is also referred to as a J7 Perx and is referenced above, was not manufactured within the state of Florida and was shipped and transported in interstate and foreign commerce.

10. Based upon the foregoing facts, I have probable cause to believe that on or about May 3, 2019, in the Middle District of Florida, COLUMBUS DONAVAN JEFFREY, did employ, use, persuade, induce, entice and coerce a minor to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, and which visual depictions were produced using materials that have been mailed, shipped and transported in and affecting interstate and foreign commerce, in violation of 18 U.S.C. § 2251(a).


ABBIGAIL BECCACCIO, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 13th day of January, 2020, at Jacksonville, Florida.


JAMES R. KLINDT
United States Magistrate Judge

EXHIBIT A

gk

SA# 19CF059019

IN THE CIRCUIT COURT OF THE FOURTH JUDICIAL
CIRCUIT IN AND FOR DUVAL COUNTY, FLORIDA

SEARCH WARRANT

IN THE NAME OF THE STATE OF FLORIDA,

TO ALL AND SINGULAR:

The Sheriff or Deputy Sheriffs of Duval County, Florida:

WHEREAS, complaint on oath and in writing supported by affidavit of credible witness which is incorporated by reference herein, to wit: Detective A. M. Arteaga of the Jacksonville Sheriff's Office, has been made to me the undersigned Circuit Court Judge in and for Duval County Florida, and

WHEREAS said facts made known to me and considered by me have caused me to certify and find that there is probable cause to believe that certain laws have been and are being violated, and that evidence of the violation of certain laws in the form of computer equipment and data, or printed or written documents and other related items described herein, are being kept in or about certain premises and the curtilage thereof and/or vehicles upon the curtilage belonging to or used by the resident(s) of said premises, in Duval County, Florida, being known and described as follows:

2154 West 16th Street, Jacksonville, Florida 32209

Description of Premises: The structure at 2154 West 16th Street, Jacksonville, Florida (hereafter the "Premises") is a single story residence. The Premises' exterior has a cinderblock finish, which is painted grey in color. There is a small front porch with black metal support posts. The Premises have the numbers "2154" displayed above the open car port and the numerals are white in color. The Premises' front door is painted red in color and there are dark blue window shutters on the front windows. The Premises' front door faces north and the driveway is located east side of the residence.

JMX

SA# _____

WHEREAS, the Court having found probable cause that a computer or other digital device capable of accessing the internet by means of service provided at or through the above described residence was knowingly used as an instrumentality of a crime and contains evidence relevant to proving a violation of the following Felony laws, to wit: **§847.0135(2), Florida Statutes**, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act," and **§827.071, Florida Statutes**, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct, and where the Premises is being occupied by **Columbus Jeffrey**, and others known and unknown, and **Columbus Jeffrey** is the registered account holder of the internet service through AT&T, provided at the Premises, this search warrant is authorized pursuant to **§933.18(6), Florida Statutes**.

NOW THEREFORE, you are hereby ordered and authorized to seize the following items, and to conduct an offsite search and analysis, or to delegate the search and analysis to an off-site computer forensic analyst, of the following items (hereinafter the "Property"):

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, personal digital assistants (PDA), 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 or child erotica, display or access information pertaining to a sexual

JMK

SA# _____

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 §847.001(4), Florida Statutes, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in §847.001(4), Florida Statutes, visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes, 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 §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.
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 §847.001(4), Florida Statutes, or any visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.
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)

fin

SA# _____

concerning the receipt, transmission, or possession of child pornography as defined in §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.

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, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
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; which may have been used to possess images and/or videos of child pornography.
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 that may be or are used to: visually depict

Jack

SA# _____

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.

12. Any and all cameras, film, videotapes or other photographic equipment that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
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 §847.001(4), Florida Statutes, or any visual depiction of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.
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 sexual conduct, as defined in §847.001(16), Florida Statutes, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access

gk

SA# _____

information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

(Paragraphs 1-15 hereinafter, the "Property")

In addition to the seizure of the abovementioned Property, the Court gives permission to seize the computer hardware (and associated peripherals) and software and to conduct an offsite analysis of the hardware and software for the evidence described, if, upon arriving at the scene, the law enforcement officers executing the search conclude that it would be impractical to search the computer hardware onsite for this evidence. The Court is aware that the recovery of data and digital evidence by a computer forensic analyst takes significant time. For this reason, the "return" inventory will be satisfied by a list of only the tangible items recovered from the premises.


NOW THEREFORE, you, with such lawful assistance as may be necessary, to include forensic computer analyst experts, are hereby commanded, in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, to enter and search the aforesaid Premises and curtilage thereof, and any vehicles thereon, or any persons located on the Premises or within the curtilage reasonably believed to be connected with said illegal activity, for the Property described in this warrant, and if the same or any part thereof be found, you are hereby authorized to seize and secure same, giving proper receipt thereof and delivering a completed copy of this warrant to the person in control of the Premises, or in the absence of any such person, leaving a completed copy where the items are found, and making a return of your doings under this warrant within ten (10) days of the date hereof, and you or your designated forensic analyst are further authorized to search the Property for evidence of the crimes described herein, and you are directed to confirm the security of said Property so it may be brought before a Court having jurisdiction of this offense to be used in the prosecution of persons violating this offense and thereafter to be disposed of according to law. In addition, during the execution of said search warrant of the Premises, law enforcement personnel are authorized to press the finger(s) (including thumbs) of any occupant

JK

SA# _____

present on the Premises at the time, to a device(s) fingerprint sensor, or present any occupant's iris or face to the device(s) camera in an attempt to unlock the device(s) for the purpose of executing the search authorized by this warrant. These device(s) will include mobile phones, tablets, laptops and/or any electronic device capable of using a biometric authentication system to unlock and access the device.

WITNESS my hand and seal this 3^d day of October, 2019.



Judge, Circuit/County Court of the Fourth
Judicial Circuit in and for Duval County, Florida

gmk

SA# 19CF059019

IN THE CIRCUIT COURT OF THE FOURTH JUDICIAL
CIRCUIT IN AND FOR DUVAL COUNTY, FLORIDA

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

BEFORE ME, Robert Dees, Judge of the Fourth Judicial Circuit, in and for Duval County, Florida, personally came Affiant Det. A. M. Arteaga 74969, a Detective with the Jacksonville Sheriff's Office, and being duly sworn, deposes and says that your Affiant has probable cause to believe that certain laws have been and are being violated, and that evidence of the violation of certain laws in the form of computer equipment and data, or printed or written documents and other related items described herein, are being kept in or about certain premises and the curtilage thereof and/or vehicles upon the curtilage belonging to or used by the resident(s) of said premises, in Duval County, Florida, being known and described as follows:

2154 West 16th Street, Jacksonville, Florida 32209

Description of Premises: The structure at 2154 West 16th Street, Jacksonville, Florida (hereafter the "Premises") is a single story residence. The Premises' exterior has a cinderblock finish, which is painted grey in color. There is a small front porch with black metal support posts. The Premises have the numbers "2154" displayed above the open car port and the numerals are white in color. The Premises' front door is painted red in color and there are dark blue window shutters on the front windows. The Premises' front door faces north and the driveway is located east side of the residence.

The above-described Premises are being used in violation of the following Felony laws: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act", and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct. This request for a search warrant is authorized pursuant to §933.18(6), Florida Statutes.

gmk

SA# _____

Jim

SA# _____

INTRODUCTION

Your Affiant is a Detective with the Jacksonville Sheriff's Office. Your Affiant has been a Police Officer with the Jacksonville Sheriff's Office for approximately five (5) years. Your Affiant is currently a Detective assigned to Internet Crimes Against Children (ICAC) investigations, and has been so assigned for four (4) months. Your Affiant's duties include taking an active role in criminal investigations that relate to the online exploitation of children. Your Affiant has received specialized training through the Office of Juvenile and Delinquency Prevention related to Internet Crimes Against Children Investigative Techniques and Undercover Chat Operations. Your Affiant has received formal training in the area of protecting children online, ICAC investigative techniques, online child pornography, and the sexual exploitation of children.

Your Affiant is a member of the North Florida Internet Crimes Against Children (ICAC) Task Force. ICAC is a national organization which provides specialized high-technology training and resources to law enforcement agencies that investigate crimes dealing with online sexual-solicitation and sexual-exploitation of children, including the collection and trading of images of child pornography. Your Affiant has an understanding of the Internet and has participated in investigations involving undercover chat sessions, child sexual-solicitation, and the receipt, transportation, distribution and possession of child pornography.

Your Affiant has investigated and/or assisted in investigations of crimes against children including: Sexual Child Abuse, Online Enticement of Children, Obscenity Directed at Minors, and Travelling with the Intent to have Sex with Minors.

Your Affiant has investigated and assisted in the investigation of matters involving the possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography.

The statements contained in this affidavit are based on your Affiant's personal knowledge, and this affidavit is being submitted for the limited purpose of securing a search warrant. Your Affiant has not included each and every fact known to him

SA# _____

concerning this investigation and has instead set forth only the facts that he believed were necessary to establish probable cause. Your Affiant has developed probable cause to believe, and does believe, that a computer or other digital device capable of accessing the internet by means of service at the above described residence or on the Premises and/or the curtilage thereof, was knowingly used by a known person(s) as an instrumentality of a crime in the commission of violations of §847.0135(2) and §827.071, Florida Statutes, related to the unlawful possession or transmission of images, movies, or visual depictions of sexual conduct or sexual performance by a child or children.

DEFINITIONS PERTAINING TO CHILD PORNOGRAPHY

1. "Child Pornography," as used herein, includes the definition in §847.001(3), Florida Statutes, which means "any image depicting a minor engaged in sexual conduct."
2. "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.
3. "Sexual conduct," as used herein, includes the definition in §847.001(16), Florida Statutes, which "means actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, or sadomasochistic abuse; actual lewd exhibition of the genitals; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being or will be committed. A mother's breastfeeding of her baby does not under any circumstance constitute "sexual conduct."
4. "Sexual performance," as used herein, means any performance or part thereof which includes sexual conduct by a child of less than 18 years of age (pursuant to §827.071(1)(i), Florida Statutes).
5. "Sexually Oriented Material," as used herein, includes the definition in §847.001(18), Florida Statutes, which "means any book, article, magazine, publication, or written matter of any kind or any drawing, etching, painting,

Jm

SA# _____

photograph, motion picture film, or sound recording that depicts sexual activity, actual or simulated, involving human beings or human beings and animals, that exhibits uncovered human genitals or the pubic region in a lewd or lascivious manner, or that exhibits human male genitals in a discernibly turgid state, even if completely and opaquely covered.”

DEFINITIONS PERTAINING TO TECHNICAL TERMS

As part of your Affiant's training, your Affiant has become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail (“e-mail”). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet through a university, an employer, or a commercial service such as an “Electronic Service Provider” or “ESP” (see definition of “Electronic Service Provider” below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit web sites and make purchases.

1. “Computer,” as used herein, includes the definition in §847.001(4), Florida Statutes, which “means 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. The term also includes: any online service, Internet service, or local bulletin board; any electronic storage device, including a floppy disk or other magnetic storage device; or any compact



SA# _____

disc that has read-only memory and the capacity to store audio, video, or written materials."

2. "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).
3. "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.
4. 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

June

SA# _____

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

5. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
6. "Electronic Service Providers (ESPs)" as used herein, ESPs, formerly known as ISPs (Internet Service Providers), are commercial organizations that are in business to provide individuals and businesses access to the Internet. ESPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ESPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ESPs typically charge a fee based upon the type of connection and volume of data, called band-width, which the connection supports. Many ESPs assign each subscriber an account name - a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a cable modem (telephone line or through a cable system) or wireless connection, the subscriber can establish communication with an ESP and can access the Internet by using his or her account name and personal password. ESPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access

JMK

SA# _____

information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ESPs servers, and other information, which may be stored both in computer data format and in written or printed record format. ESPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ESPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ESP customer is stored temporarily by an ESP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage" (18 U.S.C. §2510 (17)). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long-term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service" (18 U.S.C. §2711(2)).

7. "Internet Protocol Address (IP Address)", as used herein, every computer or device on the Internet is referenced by a unique Internet Protocol (IP) address the same way every telephone has a unique telephone number. An IPv4 address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IPv4 address is 192.168.10.102. IPv6 was created to deal with the exhaustion of the IPv4. IPv6 is the most recent version of the Internet Protocol (IP). An example of an Ipv6 is 3ffe:1900:4545:3:200:f8ff:fe21:67cf, but methods to abbreviate this full notation exist. Each time an individual has accessed the Internet, the computer from which that individual initiated access is assigned an IP address. A central authority provides each ESP a limited block of IP addresses for use by that ESP's customers or subscribers. Most ESPs employ dynamic IP addressing, that is they allocate any unused IP addresses at the time of initiation of an Internet session each time a customer or subscriber has accessed the Internet. A dynamic IP address is reserved by an ESP to be shared among a group of computers over a period of time. The

JMC

SA# _____

- ESP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Another method of IP addressing is known as a Static IP address. A Static IP address is an IP address that does not change over a period of time.
8. "Log File", as used herein, log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
 9. "Metadata", as used herein, data contained in a file that is not usually associated with the content of a file but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it and the date the image was taken.
 10. "Uploading", as used herein, uploading is transmission in the other direction: from one computer to another computer. From an Internet user's point-of-view, uploading is sending a file to a computer that is set up to receive it.
 11. "Downloading", as used herein, downloading is the transmission of a file from one computer system to another. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.
 12. "Domain Name", as used herein, domain names are common, easy to remember names associated with an Internet Protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32.

Jhu

SA# _____

13. "Compressed File", as used herein, a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.
14. "Hash Value", as used herein, a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data.
15. "Image or Copy", as used herein, an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

COMPUTERS AND CHILD PORNOGRAPHY

Based upon your Affiant's training and experience, as well as consultation with other experienced law enforcement officers and computer forensic examiners, your Affiant knows 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 a significant amount of skill in order 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.

The development of computers has radically changed the way that child pornographers obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a

Jan

SA# _____

device known as a scanner. Moreover, with the advent and widespread use of digital cameras, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding thousands 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.

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.

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

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

jmk

SA# _____

videos can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs."

Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon his training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, your Affiant knows that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to electronic communication, 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

Based upon your Affiant's training and experience, as well as conversations with other experienced law enforcement officers, your Affiant knows that searches and seizures of evidence from computers commonly require Forensic Examiners 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:

1. Computer storage devices (e.g., hard drives, compact discs ("CDs"), diskettes, tapes, and others) can store the equivalent of thousands of pages of information.

SA# _____

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.

2. 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. 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.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

Based on your Affiant's experience, training, and consultation with other experienced law enforcement officers who investigate cases involving the sexual exploitation of children, your Affiant knows that certain common characteristics are often present in individuals who collect child pornography. Your Affiant has 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 his training and experience, and conversations with other experienced law enforcement officers in the area of investigating cases involving sexual exploitation of children, your Affiant knows that the following traits and characteristics are often present in individuals who collect child pornography:

Jan

SA# _____

1. 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.
2. Many individuals who collect child pornography collect sexually oriented 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 rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Such individuals often do not destroy these materials.
3. 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 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.
4. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.
5. 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

ju

SA# _____

traded with other likeminded 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. Based on his training and experience, as well as his conversations with other experienced law enforcement officers, your Affiant knows that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often continue to maintain and/or possess the items.

The known desire of such individuals to retain child pornography, coupled with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and child 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.

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

Your Affiant makes this affidavit in support of a search warrant for the Premises located at 2154 West 16th Street, Jacksonville, Florida, believed to currently be occupied by Columbus Jeffrey.

On September 17, 2019, the North Florida Internet Crimes against Children (ICAC) Task Force received a Cyber Tip Report from the National Center for Missing and Exploited Children (Reports #53500239 and 56041995). The National Center for Missing and Exploited Children (NCMEC) Cyber Tip Line is an online reporting mechanism for cases of child sexual exploitation including child pornography, online enticement of children for sex acts, molestation of children outside the family, sex tourism of children, child victims of prostitution, and unsolicited obscene material sent to a child. NCMEC staff reviews reports, sometimes doing basic analysis work, and then distributes the Cyber Tip Report

SA# _____

to the appropriate investigatory agencies for review. This Cyber Tip Report came from Tumblr, Inc. (hereinafter "Tumblr"). Tumblr is a microblogging and social networking website where images can be shared and distributed through the websites blogging capabilities and messaging. In reference to the aforementioned Cyber Tip Report submitted through Tumblr, the associated Tumblr account with the Email Address of "columbusjeffrey@gmail.com," Screen/Username "hideme1977", ESP User ID of "168404581", and an IP Address of 76.245.76.84 was used to upload five (5) child pornography images and three (3) child pornography videos.

Your Affiant personally viewed the images in the Cyber Tip Report and confirmed that they met the definition of child pornography, pursuant to §847.001(3), Florida Statutes. The following are descriptions of one of the child pornography images and one of the videos viewed by your Affiant:

IMAGE TITLE: 184099761061_0_npf_video.mp4

Hash: 5e1e57a292479d88a06900ec2b4161f1

DESCRIPTION: This video depicts a pubescent male child, approximately 13-15 years old. The child is seen holding an erect penis and is performing oral sex on the subject.

IMAGE TITLE: 184146549751_0_inline_image.jpg

HASH: df6df71fd9190d037ba06e78c262cd9d

DESCRIPTION: This image depicts a prepubescent male child, approximately 10-12 years old. The child is bending over on a bed naked with his genital and buttocks area facing the camera. This appears to be the focal point of the entire picture.

A search of the IP address revealed that it belonged to ATT U-verse in Jacksonville, Florida.

On October 2, 2019, Your Affiant caused a Fourth Judicial Circuit Subpoena Duces Tecum to be served to AT&T Internet Services requesting all available account subscriber information for the above referenced IP address on the specific date and time the Tumblr

SA# _____

account, containing the child pornography, was accessed. On October 2, 2019, Your Affiant received a response from AT&T Internet Services disclosing the following information for the above referenced IP address:

Jnu

SA# _____

Subscriber Information

Contact Name: Columbus Jeffrey
Service Address: 2154 W. 16th St.
Jacksonville, FL 32209
Cell Phone #: (941) 527-7441
Billing: AT&T
Account ID: 291573451
Account Status: Active
Email: columbusjeffrey@gmail.com
IP Address: 76.245.76.84

During the course of the investigation your Affiant was able to determine that the residence and power come back to Columbus Jeffrey. The subject's Florida Driver's License also lists 2154 West 16th Street as his address.

On October 3, 2019, your Affiant personally observed and took photographs of the Premises located at 2154 West 16th Street, Jacksonville, Florida. The photographs are consistent with the aforementioned description of the Premises.

CONCLUSION

The above information leads your Affiant to believe that a computer or other digital media capable of securing Internet access at the above described Premises, residence, curtilage or related vehicles thereon, was knowingly used by a known person/s as an instrumentality of a crime or as a means by which a Felony was committed, (§933.18(6), Florida Statutes). The following Felony laws were violated through the use of said computer: §847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act," and §827.071, Florida Statutes, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct.

Your Affiant hereby requests the Court's permission to seize the following items, and to conduct a search and analysis, or to delegate the search and analysis to a

June

SA# _____

computer forensic analyst, on-scene or off-site at another secure location, of the following items (hereinafter the "Property"):

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, personal digital assistants (PDA), 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 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 §847.001(4), Florida Statutes, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in §847.001(4), Florida Statutes, visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes, or child erotica.



SA# _____

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 §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct as defined in §847.001(16), Florida Statutes.
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 §847.001(4), Florida Statutes, or any visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.
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 §847.001(4), Florida Statutes, or visual depictions of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.
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, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
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

John

SA# _____

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; which may have been used to possess images and/or videos of child pornography.
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 that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
12. Any and all cameras, film, videotapes or other photographic equipment that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.
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 §847.001(4),

JK

SA# _____

Florida Statutes, or any visual depiction of minors engaged in sexual conduct, as defined in §847.001(16), Florida Statutes.

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 sexual conduct, as defined in §847.001(16), Florida Statutes, that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

(Paragraphs 1-15 hereinafter referred to as the "Property")

Your Affiant believes that the above items are being kept at 2154 W. 16th Street, Jacksonville, Florida and are being used in violation of the laws of the State of Florida, and constitute evidence of, or evidence relevant to proving, a violation of the laws of the State of Florida, to wit:

Section 847.0135(2), Florida Statutes, prohibiting possession of child pornography under the: "Computer Pornography and Child Exploitation Prevention Act", and **§827.071, Florida Statutes**, prohibiting the sexual performance of a child and the creation, possession or promotion of an image of such conduct.

Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time, and much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the

Jur

SA# _____

premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

WHEREFORE, your Affiant makes this affidavit and requests the issuance of a Search Warrant in due form of law commanding the Sheriff of the Jacksonville Sheriff's Office, or any of his duly constituted officers, with any proper and necessary assistance, including the assistance of a trained computer forensic analyst, to search the above described Premises and the curtilage thereof and/or the vehicle(s) on the curtilage thereof, or persons located within the Premises and the curtilage reasonably believed to be connected with said illegal activity, for the said Property heretofore described, and to search and analyze said Property described above or delegate, either on premises or off-site, such analysis and to seize and safely keep same, either in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, in order that the evidence may be procured to be used in the prosecution of such person or persons who have unlawfully used, possessed, or are using or possessing the same in violation of the laws of the State of Florida.

Det [Signature] 74909

Detective A.M. Arteaga, Affiant
Jacksonville Sheriff's Office
Internet Crimes Against Children Task Force

Sworn to and subscribed before me in Duval County, Florida, this 30th day of October, 2019. The Affiant/Co-Affiant is [] personally known or [☒] identified by JSO ID.

[Signature]

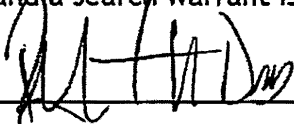
Judge, Circuit/County Court of the Fourth
Judicial Circuit in and for Duval County, Florida

The above application for Search Warrant coming on to be heard and having examined the applications under oath and the above sworn affidavit set forth and other facts and thereupon being satisfied that there is probable cause to believe that the grounds set

dm

SA# _____

forth in said Application and the facts do exist and that the law is being violated, I so find, and a search warrant is hereby allowed and issued.



Judge, Circuit/County Court of the Fourth
Judicial Circuit in and for Duval County, Florida

