

# UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America )

v. )

Case No. )

3:15-mj-1217-MCR )

KYLE ADAM KIRBY )

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 between 12/24/14 through 10/22/15 in the county of Suwannee in the Middle District of Florida, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2)	possession of child pornography.

This criminal complaint is based on these facts:

See attached affidavit.

CERTIFIED A TRUE COPY  
 SHERYL V. LOESCH, CLERK  
 U.S. DISTRICT COURT  
 Deputy Clerk

Continued on the attached sheet.

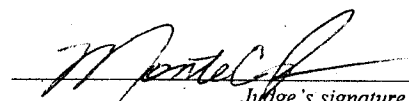
  
 Complainant's signature

Special Agent Abbigail Beccaccio, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/27/15

  
 Judge's signature

City and state: Jacksonville, Florida

Monte C. Richardson, U.S. Magistrate Judge

Printed name and title

## AFFIDAVIT

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

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 the Forensics and Technology Unit Supervisor with the Orlando Police Department for approximately eight 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 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 possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography. I have been involved in searches pertaining to the possession, collection, production, and/or transportation of child pornography through either the execution of search warrants or through the subject providing written consent to permit a search. I have served as the affiant for federal search warrants and federal criminal complaints in cases involving child exploitation offenses. I have also conducted undercover online investigations of individuals who use the internet to engage in the sexual exploitation of children.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children, including violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, as well as Florida state statutes that criminalize the production, receipt, transportation, and possession of child pornography, that is, visual depictions of minors engaged in sexually explicit conduct. I am a member of a local child pornography task force comprised of the FBI, the Florida Department of Law Enforcement, the Jacksonville Sheriff's Office, the St. Johns County Sheriff's Office, and the Columbia County Sheriff's Office, among other agencies. We routinely share information involving the characteristics of child pornography offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers. This affidavit is being submitted for the limited purpose of establishing probable cause for the filing of a criminal complaint, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that KYLE ADAM KIRBY has committed a violation of Title 18, United States Code, Sections 2252(a)(4)(B), that is, possession of child pornography.

4. This affidavit is made in support of a complaint against KYLE ADAM KIRBY, that is, during the period from on or about December 24, 2014 through on or

about October 22, 2015, at Live Oak, in Suwannee County, in the Middle District of Florida, KYLE ADAM KIRBY did knowingly possess one or more matters which contained visual depictions which were produced using materials which have been shipped and transported in or affecting interstate or foreign commerce, that is, a Fujitsu computer hard disk drive, serial number K62AT8C2819f, manufactured in Thailand, the production of which involved the use of minors engaging in sexually explicit conduct, which visual depictions were of such conduct, and which visual depictions are specifically identified in the computer file, among others, titled "babyj – rca2.mpg.jpg," in violation of Title 18, United States Code, Sections 2252(a)(4)(B) and 2252(b)(2).

5. On October 21, 2015, I applied for and obtained a federal search warrant for the residence located at 530 Westmoreland Street SE, Live Oak, Florida 32064. This warrant was issued by United States Magistrate Judge Monte C. Richardson in Case No. 3:15-mj-1210-MCR. A certified copy of the application and affidavit for this search warrant and the warrant itself are attached as Composite Exhibit A, and the facts and information contained therein is hereby incorporated by reference herein.

6. On October 22, 2015, I, together with other law enforcement officers, traveled to Live Oak for the purpose of executing that federal search warrant at the residence located at 530 Westmoreland Street SE, Live Oak, Florida 32064. I did not personally participate in the execution of the search warrant because I went to the Live Oak Police Department for the purpose of making contact with KIRBY.

7. Once at the Live Oak Police Department (LOPD), I met with the LOPD Chief of Police Alton K. Williams. Subsequently, and in substance and among other things, I learned the following information:

a. Chief Williams had been contacted on October 21, 2015, by Assistant Special Agent in Charge (ASAC) Kacey D. Gabriel, to schedule a meeting. Chief Williams had been advised the Federal Bureau of Investigation wished to meet with him regarding a search warrant that was to be executed in Live Oak on October 22, 2015. The meeting was scheduled for 9:00 a.m. on October 22, 2015.

b. I attended the meeting with Special Agent Lawrence S. Meyer and ASAC Kacey D. Gabriel. During the meeting, Chief Williams was told the search warrant was going to be executed at the residence of LOPD Sergeant KYLE KIRBY in Live Oak, Florida.

c. Chief Williams advised that he would cooperate with the FBI in every aspect of the investigation. Chief Williams further stated the FBI was welcome to search and inspect any of the LOPD's owned items in KIRBY's possession.

d. Chief Williams stated that he has known KIRBY since Chief Williams was a School Resource Officer in Columbia County (FL) and KIRBY was a student.

e. Chief Williams agreed to have KIRBY called to the station and remove his duty firearm from him. Chief Williams advised that KIRBY would agree to speak with the agents. Chief Williams requested to brief his Deputy Chief and another Live Oak employee on the situation at this time.

8. After a short period of time, ASAC Kacey D. Gabriel and I were invited to rejoin Chief Williams in his office with Deputy Chief (DC) Joe Daly and Investigator Larry Rogers. Subsequently, and in substance and among other things, I learned the following information:

a. While in Chief Williams' office, DC Daly stated that he was receiving a phone call from KIRBY.

b. DC Daly answered the call, greeted KIRBY, and asked KIRBY if KIRBY was out on patrol. KIRBY provided a response, which was not audible to me, and DC Daly then asked KIRBY to "swing by" the station when KIRBY had a moment. KIRBY again provided a response that was not audible to me, and DC Daly stated that he would see KIRBY shortly.

c. Following the phone call, DC Daly told Chief Williams that KIRBY would come to the station shortly.

d. DC Daly and Investigator Larry Rogers left the office at this time.

9. After a brief period of time, KIRBY arrived at the LOPD office and knocked on Chief Williams' office door. Subsequently, and in substance and among other things, I observed the following because I was present in the Chief's office:

a. KIRBY entered the office and took the seat in the chair directly in front of Chief Williams' desk.

b. Chief Williams told KIRBY that he (KIRBY) would be on immediate suspension pending an investigation into "child porn" and requested that KIRBY

surrender his duty firearm, badge and identification card. KIRBY surrendered these items without incident.

c. Chief Williams then told KIRBY that the agents, who were present in the room, wished to speak with him in the conference room.

10. I then followed KIRBY from Chief Williams's office into the unlocked conference room with ASAC Gabriel.<sup>1</sup> Subsequently, the following events took place:

a. I shook KIRBY's hand and identified myself. I told KIRBY that, placed in the same situation, he would understand my need to search him for a secondary weapon. KIRBY agreed and stated that he did not have one and raised his pant legs for me to view. I then asked KIRBY to sit down at the conference table so I could begin speaking with him. KIRBY consented and took a seat opposite me at the conference room table.

b. I asked KIRBY how long he had worked for the LOPD, and he responded since 2003. KIRBY clarified that he left briefly for a period and came back in 2006. I advised KIRBY that he was not under arrest, was free to leave, and that a federal search warrant was being executed at his residence.

c. I told KIRBY that I wished to speak with him further regarding why the FBI was in Live Oak and explained that, in an abundance of caution, I intended to advise him of his constitutional rights. I then read from the FBI FD-395 "Advice of Rights" form to KIRBY. I then passed the form to KIRBY, asked him to read the

---

<sup>1</sup> I know that LOPD personnel requested KIRBY's house key prior to KIRBY coming into the LOPD conference room. KIRBY advised that his house key was in his LOPD patrol car on a key ring and verbally authorized its use to avoid any property damage that might be caused by forced entry to his residence.

"consent" portion if he agreed to speak with me. At that point, KIRBY advised that he needed to speak to an attorney first. I told KIRBY that I could no longer speak with him at this time.

d. Despite my termination of the interview, KIRBY asked if he could go to his residence and I told KIRBY that he would not be allowed into his residence until the completion of the execution of the search warrant. KIRBY twice requested a copy of the search warrant but was told that a copy of the search warrant along with a FD-597 form (FBI Receipt for Property form) would be left in his residence at the completion of the search.

e. KIRBY asked if he could stand outside of his residence during the search, and Task Force Officer (TFO) Jimmy Watson, who had entered the conference room while I was advising KIRBY of his constitutional rights, told KIRBY that KIRBY was allowed to be present outside his residence, but that his presence may draw undue attention to the incident.

f. I told KIRBY that I would be in close proximity, if he decided that he wished to speak to me further without an attorney. I also advised KIRBY again that he was not under arrest and was free to leave, but that Chief Williams wished to speak with him prior to his departure. ASAC Gabriel, TFO Watson and I then left the room at this time. I verified upon exiting that the conference room door was unlocked and that KIRBY was physically able to exit the door if he wished.

11. Following my conversation with KIRBY, TFO Watson and I waited outside at the rear of the LOPD station. Chief Williams was present with us during some of this



time and I know that Chief Williams, not acting at my direction, went in to see KIRBY and had a brief discussion with him.

12. During this time, SA Meyer advised me by telephone that the search team had not located any computers at KIRBY's residence.

13. During KIRBY's interview, I observed that KIRBY had a cellular phone on his person, clipped to the front of his duty belt, in plain view. After KIRBY's discussion with Chief Williams, I observed as TFO Watson returned to the conference room where KIRBY was waiting. TFO Watson told me that KIRBY was on the phone when TFO Watson entered the conference room. TFO Watson allowed KIRBY to complete his phone call and then asked KIRBY to provide the phone to TFO Watson. KIRBY provided the phone to TFO Watson, who took custody of the phone.

14. I was then advised that the search team was concluding the search of KIRBY's residence. Subsequently, and in substance and among other things, SA Meyer advised me of the following:

a. SA Meyer left a copy of the inventory of items seized pursuant to the search warrant was documented on FBI FD-597. Seized during the course of the search but not included within the scope of the warrant were several firearms and badges which were the property of LOPD. No computers or computer media was found at the residence.

b. Several additional firearms and ammunition were also seized at the request of LOPD Chief Williams based on safety concerns. These items were

documented on an FBI FD-886 "Evidence Collected Log." Also taken by the LOPD detectives on scene, and not documented on the FD-886 form were several LOPD uniforms that are the property of the LOPD and additional ammunition.

15. Later on October 22, 2015, TFO Watson applied for and obtained a state search warrant for KIRBY's cell phone, a black Samsung Galaxy Note 3 Verizon 4G LTE device with Lion Screensaver. This warrant was issued by Circuit Court Judge David W. Fina in Live Oak, Florida.

16. I was then advised by SA Meyer and SA Wood that a search based on consent by LOPD personnel and authorized by Chief Williams was conducted of a marked Dodge Magnum patrol car used by KIRBY and owned by the LOPD, Florida City tag 110861. Subsequently, and in substance and among other things, I was advised of the following information:

a. LOPD Detective Jason Roundtree, acting at the direction of Chief Williams, authorized the FBI to take possession of a LOPD Panasonic CF-52 laptop computer, serial number 9DTYA55692, that had been obtained from within the patrol car that KIRBY had used. This was authorized pursuant to LOPD policy in order to conduct an inspection and search of this laptop computer at the FBI Jacksonville Field Office.

b. At that time, LOPD Detective Roundtree executed an FBI FD-26 "Consent to Search" form that authorized this inspection and search.

17. I have reviewed the LOPD's "Electronic SOP Policy Manual Sign in Sheet" and LOPD's "Computer Assignment Record," provided to me by LOPD personnel and

and a review of these documents shows the following:

- a. On June 9, 2009, KIRBY signed for a Panasonic PF52 computer, serial number 9DTYA55692, with City asset tag 02731, that was assigned to him.
- b. On March 16, 2012, KIRBY initialed the LOPD "Electronic SOP Policy Manual Sign in Sheet."
- c. On July 22, 2013, KIRBY signed a sheet titled "Policy Revision: Computers/Electronic mail SOP-806", "Instructor: Lt. Keith Davis", "1 Hour Training" that was attached to a document titled "SOP-806, Computers/Electronic Mail", "Effective: 08-01", "Review: August/Yearly", "COMPUTERS/ELECTRONIC MAIL" (the "LOPD SOP policy. This 11-page document shows on its face that it was "Revised 07/13".

18. I have reviewed the LOPD SOP policy that provides, in pertinent part, as follows:

- a. On pages 806-3 and 806-4, under the headings "Mobile Data Computers (MDC's or notebook)", "Responsibilities", paragraph III.D.1.b. states, in pertinent part, that "They [supervisors] shall conduct inspections of the notebook computers assigned to their personnel at least once a month to assure that they are being maintained properly."
- b. On page 806-6, under the headings "Mobile Data Computers (MDC's or notebook)", "Use Of Notebook Computers", paragraph III.D.2.c.(5) states, in pertinent part, that "[d]epartment notebook computers will be subject to inspection by supervisors."

c. On page 806-9, under the headings "Mobile Data Computers (MDC's or notebook)", "Inspections", paragraph III.D.5.a. states, in pertinent part, "Notebook computers which are the property of the Live Oak Police Department shall be subject to routine periodic inspection by supervisors, Administrative Services Division Commander and Staff Inspection Members. The computers will be inspected for routine care and maintenance purposes, as well as to insure the integrity of the software that is loaded in them. Members should be aware that all files contained in the Departmental computers are subject to review by personnel conducting said inspections."

19. On October 26, 2015, I was advised by FBI SA John Wood, a certified computer forensic examiner, that a preliminary search of KIRBY's cell phone, a black Samsung Galaxy Note 3 Verizon 4 G LTE device with Lion Screensaver, did not locate any images or videos depicting child pornography, but this forensic examination is still ongoing.

20. Also on October 26, 2015, SA Wood advised me that he had conducted a preliminary forensic review of the laptop computer owned by the LOPD, used by KIRBY, and obtained by consent from the LOPD on October 22, 2015, that is, the Panasonic CF-52 laptop computer, serial number 9DTYA55692, that contained a Fujitsu computer hard disk drive, serial number K62AT8C2819f, manufactured in Thailand. SA Wood advised me, in substance and among other things, of the following:

a. References to the internet protocol (IP) addresses used to obtain the search warrant (see Composite Exhibit A), that is, IP address 66.177.66.109 and IP address 73.148.219.9, were found on the Fujitsu computer hard disk drive contained in

the Panasonic CF-52 laptop computer. Both IP addresses were found in numerous locations on the computer, including the hibernation file, showing that the computer had been hibernating, or in "sleep mode," while accessing those IP addresses.

b. Searches were conducted for any evidence of graphic files containing depictions of child pornography. Located in the file path "C:/Documents and Settings/Kyle/My Documents/Downloads" was a "thumbs.db"<sup>2</sup> file folder that contained at least 87 thumbnail image files that either depicted minor children engaged in sexually explicit conduct or that had with titles indicative of child pornography or child exploitation, including one particular image file titled "babyj – rca2.mpg.jpg"<sup>3</sup>.

c. The original files, whether image or video files, had been deleted, but the fact that the thumbnails existed shows not only that the original graphic or video files did exist and were contained at one time in that folder, but they were viewed by the computer user<sup>4</sup> using "Windows Explorer" in thumbnail view on one or more occasions. That file path, "C:/Documents and Settings/Kyle/My Documents/Downloads," was also shown to be the default download location for the "uTorrent.exe" application.

---

<sup>2</sup> Based on my training and experience, as well as my conversations with SA Wood, I know that a thumbs.db file is a Windows XP system file that is created when a user views a folder in thumbnail view. When the thumbs.db file is generated, a "screen shot," or a "thumbnail" image is pulled from the graphic file contained within the folder and is presented to the computer user as a representation of the original file so that the user can easily identify, reference and otherwise keep track of it.

<sup>3</sup> Based on my training and experience, as well as my conversations with SA Wood, I know that the ".jpg" is automatically placed as a suffix onto the original file name (that ended in ".mpg") to denote that the "thumbnail" is an image, or the first "frame" of the original video.

<sup>4</sup> I have probable cause to believe that this computer user was KIRBY.

d. A part of the thumbs.db file is the catalog stream. A catalog stream is a listing of the thumbnail file names contained inside the thumbs.db file directory. This catalog stream also contains a modified date for each file. The catalog file contained in this thumbs.db showed that the file named "babyj – rca2.mpg.jpg" had a modification date of 12/24/2014 at 06:23 AM (UTC) which is 01:23 AM Eastern. This time stamp corresponds to the time that the file was written (or downloaded) to KIRBY's computer.

21. I also reviewed the investigative history of this case, including certain logs showing dates and time that undercover law enforcement officers connected to the host computer using IP address 66.177.66.109, which as set forth herein and in the attachment, and that resolved back to KIRBY's residence. This review revealed that on December 24, 2014, between the hours of 1:05 AM and 1:39 AM, an undercover officer was able to connect to the host computer, which was using IP address 66.177.66.109 at the time, and the user of this host computer was sharing several files, including a video titled "babyj – rca2.mpg."

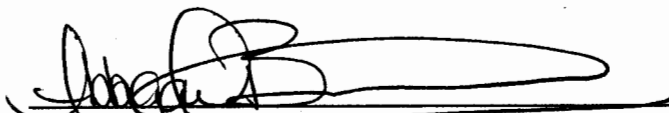
22. SA Wood also advised me that several artifacts were found on the Fujitsu computer hard disk drive in the LOPD Panasonic laptop computer used by KIRBY that showed, among other things, the presence of a "lnk" file (also referred to as a shortcut file) for the "babyj – rca2.mpg.jpg" file. This "lnk" file once existed in KIRBY's recent folder and shows that the file was viewed by the computer user, whom I have probable cause to believe was KIRBY, on one or more occasions.

23. Also on October 26, 2015, I viewed the file titled "babyj – rca2.mpg.jpg" that was found on the Fujitsu computer hard disk drive in the LOPD Panasonic computer used by KIRBY. I recognize this image as part of a video depicting a known series of child pornography, that is, the "Baby J" series. This image depicts a close up view of the lower abdomen, genitalia, and thighs of a female toddler. The focal point of this image is the genitalia of the minor child, and it depicts the lascivious exhibition of the child's genitalia. Based on this review, I believe that this image constitutes a visual depiction of a minor engaged in sexually explicit conduct as set forth in Title 18, United States Code, Section 2256. I also viewed several other thumbnail images contained in the "Downloads" folder on the Fujitsu computer hard disk drive in the LOPD Panasonic computer used by KIRBY that depicted minors engaged in sexually explicit conduct.

24. On October 27, 2015, SA Wood further advised me that during his forensic review of the Fujitsu computer hard disk drive in the LOPD Panasonic computer used by KIRBY, he reviewed the history of the Chrome internet browser that used the Bing search engine. This review showed that the user, whom I have probable cause to believe was KIRBY, had conducted internet searches using terms, among others, including "10Yo Girl PTHC Alicia," "My 10Yo Daughter," "PTHC 5Yo," and "Real JB Teen Gallery Pics". Based on my training and experience, I know that the term "PTHC" is a common search term used by individuals seeking child pornography on the internet. I also know that such individuals also often use child age-related terms such

as "5Yo" (5 years old) and "10Yo" (10 years old) to search for child pornography that suits their particular age preference and sexual interest.

25. Based upon the foregoing facts, I have probable cause to believe that during the period from on or about December 24, 2014 through on or about October 22, 2015, at Live Oak, in Suwannee County, in the Middle District of Florida, KYLE ADAM KIRBY, did knowingly possess one or more matters which contained visual depictions which were produced using materials which have been shipped and transported in or affecting interstate or foreign commerce, that is, a Fujitsu computer hard disk drive, serial number K62AT8C2819f, the production of which involved the use of minors engaging in sexually explicit conduct, which visual depictions were of such conduct, and which visual depictions are specifically identified in the computer file, among others, titled "babyj - rca2.mpg.jpg," in violation of Title 18, United States Code, Sections 2252(a)(4)(B) and 2252(b)(2).

  
ABBIGAIL BECCACCIO, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this  
27<sup>th</sup> day of October, 2015, at Jacksonville, Florida.

  
MONTE C. RICHARDSON  
United States Magistrate Judge



# UNITED STATES DISTRICT COURT

for the  
Middle District of Florida

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*

a residence located at 530 Westmoreland Street SE  
Live Oak, Florida, 32064, more particularly  
described in Attachment A

Case No. 3:15-mj-1210-MCR

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:  
a residence located at 530 Westmoreland Street SE, Live Oak, Florida, 32064, more particularly decribed in Attachment A.

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

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

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

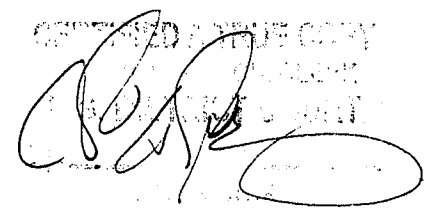
The search is related to a violation of:

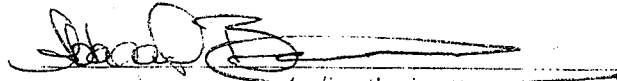
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 2252 & 2252A	Receipt and possession of child pornography.

The application is based on these facts:

See attached Affidavit.

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

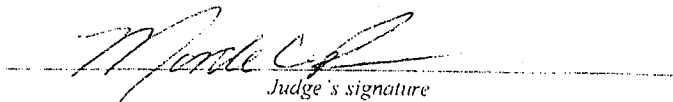
CERTIFIED TRUE COPY  
  
 FEDERAL BUREAU OF INVESTIGATION  
 U.S. DEPARTMENT OF JUSTICE

  
 Applicant's signature

Federal Bureau of Investigation Special Agent Abigail Beccaccio  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 10/21/15

  
 Judge's signature

City and state: Jacksonville, Florida

Monte C. Richardson, United States Magistrate Judge  
 Printed name and title

## AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

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 the 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 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 possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography. I have been involved in searches pertaining to the possession, collection, production, and/or transportation of child pornography through either the execution of search warrants or through the subject providing written consent to permit a search.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children, which constituted violations of Title 18, United States Code, Sections 2252 and 2252A, as well as Florida state statutes which

criminalize the possession, receipt and transmission of child pornography, that is, visual images depicting minors engaged in sexually explicit conduct.

3. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe evidence of violations of Title 18, United States Code, Sections 2252 and 2252A, is present in the residence and items to be searched.

#### **STATUTORY AUTHORITY**

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

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

b. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18

U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

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

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(3) prohibits a person from knowingly reproducing child pornography for distribution through the mails or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

e. The internet is a facility of interstate commerce.

#### **DEFINITIONS**

5. The following definitions apply to this Affidavit:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and

of themselves, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

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

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

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

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

any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic

or magnetic storage devices such as floppy diskettes, hard disk drives, CD-ROMs, digital video disks (DVDs), "smart" phones such as an Apple iPhone, electronic tablets such as an Apple iPad, personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, USB or "thumb" drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

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

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.



## COMPUTERS AND CHILD PORNOGRAPHY

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

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

8. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, images and videos can now be transferred directly from a digital

camera onto a computer using a connection known as a USB cable or other device.<sup>1</sup> Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

10. 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.

11. 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

---

<sup>1</sup> FBI SA Lawrence S. Meyer has advised me of a 2007 case filed in the Jacksonville Division of the Middle District of Florida in which he executed a federal search warrant at a residence and several computer hard disk drives were seized. Many images and videos of child pornography were discovered on these hard disk drives. Forensic analysis of these hard disk drives revealed that the owner (defendant) had converted 15-year-old Polaroid photographs depicting child pornography into digital images by scanning them onto his computer. Moreover, the analysis revealed that the owner (defendant) had made VHS videotapes containing child pornography, and then years later displayed them on a large flat screen monitor and filmed the monitor with a digital camera. Thus, the owner (defendant) successfully converted traditional photos and VHS videos into digital photographs and videos that could be stored and easily traded over the Internet.

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.

12. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, *i.e.*, by saving an email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also be retained unintentionally, *e.g.*, traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to

electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains P2P software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

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

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

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

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system, which includes the use of data search protocols, is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased,<sup>2</sup> 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**

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

---

<sup>2</sup> Based on my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that computer forensic techniques can often recover files, including images and videos of child pornography, that have long been "deleted" from computer media by a computer user.

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

b. Many individuals who collect child pornography also collect other sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not meet the legal definition of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest in children and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding

comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other like-minded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. These individuals may protect their illicit materials by passwords, encryption, and other security measures; save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted; or send it to third party image storage sites via the Internet. Based on my training and experience, as well as my conversations with other experienced law enforcement officers who conduct child exploitation investigations, I know that individuals who possess, receive, and/or distribute child pornography by

computer using the Internet often maintain and/or possess the items listed in Attachment B.

15. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials. For example, during the course of an investigation that I conducted in 2007 in the Middle District of Florida, the subject had his residence searched pursuant to a federal search warrant and his computer and digital storage media seized by the FBI. The search of his computer and other computer storage media revealed the subject knowingly possessed several thousand images of child pornography. The subject retained an attorney and both were made aware of the ongoing investigation into the subject's commission of federal child pornography offenses. Approximately two months later, the subject was arrested on federal child pornography possession charges. After the subject's arrest, the FBI obtained a laptop computer owned by the subject's employer but possessed and used by the subject both before and after the execution of the search warrant at his residence. Subsequent forensic examination of this computer revealed that the subject had downloaded, possessed and viewed images of child pornography numerous times *after* the execution of the search warrant and before his arrest.

**PEER-TO-PEER (P2P) FILE  
SHARING AND SHA1 VALUE FILE IDENTIFICATION**

16. Peer-to-peer file sharing ("P2P") is a method of communication available to Internet users through the use of special software. The software is designed to allow



users to trade digital files through a worldwide network that is formed by linking computers directly together instead of through a central server. Computers that are part of this network are referred to as "peers" or "clients." There are several different software applications that can be used to access these networks, but these applications operate in essentially the same manner. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files over the internet.

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

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

uploading to the internet is termed a "seeder." Using the BitTorrent protocol, several basic computers, such as home computers, can replace large servers while efficiently distributing files to many recipients.

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

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

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

user's computer or on an external storage media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user.

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

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

24. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. The ICAC Task

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

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

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

26. I make this affidavit in support of a search warrant for the residence located at 530 Westmoreland Street SE, Live Oak, Florida 32064 that I believe to be currently occupied by Kyle Kirby (date of birth 09/02/1980) . This affidavit is based on information provided to me both verbally and in written documentation from other law enforcement officers and personnel, including FBI Task Force Officer (TFO) Jimmy Watson, as well as through investigation that I personally conducted as set forth herein.

FBI TFO Jimmy Watson has personally observed the premises, and provided me with a written description of the premises, and this description is set forth in Attachment A. I also have reviewed digital photographs of the residence taken by TFO Watson and provided to me on October 15, 2015, and the photographs are consistent with the description as set forth in Attachment A.

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

28. FBI Task Force Officer (TFO) Jimmy Watson has advised me of and provided me with the following information, some of which was set forth in written documentation that I have reviewed. On April 16, 2015, TFO Watson began an undercover operation to identify persons using the BitTorrent P2P network on the internet to receive, traffic in, share and/or distribute images and videos depicting child pornography. I know that TFO Watson has received training in the operation and use of the BitTorrent P2P network, as well as certain law enforcement techniques used to investigate users on this network. TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 66.177.66.109 had previously

been associated with certain Files of Interest (FOI)<sup>3</sup> by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

29. FBI TFO Watson has advised me of and provided me with the following information, some of which was set forth in written documentation, which I have reviewed. On April 16, 2015, TFO Watson was able to connect to a computer using the IP address 66.177.66.109, however, he was not able to download enough pieces of any files that were sufficient for viewing. On May 6, 2015, TFO Watson learned that Investigator Ken Lakatis of the Citrus County Sheriff's Office may have been able to download files from the IP address 66.177.66.109. TFO Watson sent Investigator Lakatis an email who advised that he had made downloads from a computer using the IP address in question and would send TFO Watson the records on a disc via United States Postal Service. TFO Watson received this disc on or about May 14, 2015.

30. TFO Watson reviewed the disc after receiving it and subsequently reviewed it with me on June 12, 2015, and we learned the following information from the documentation received from Investigator Lakatis:

a. On April 16, 2015, Investigator Lakatis was investigating host computers located in Florida that were actively sharing child pornography on the

---

<sup>3</sup> Based on my training and experience, I know that the term "File(s) of Interest" refers to digital video and/or image files that depict child pornography and/or child erotica. These FOIs have previously been encountered, viewed, and catalogued by law enforcement personnel and/or staff working in and/or with ICAC task forces around the country. The descriptions and unique SHA-1 values of these FOIs are posted by ICAC investigators to the secure ICAC website for use by other ICAC trained online undercover investigators in confirming whether particular files in their respective investigations constitute child pornography or child erotica. As a law enforcement officer who specializes in the investigation of crimes against children, I have access to this secure ICAC website and have experience using it to identify and classify images and videos of suspected child pornography.

BitTorrent network. Through the use of specialized law enforcement software, Investigator Lakatis was able to determine that a host computer using IP address 66.177.66.109 had previously been associated with certain FOI by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

b. On April 16, 2015, Investigator Lakatis was able to directly connect to the host device using IP address 66.177.66.109. The device reported that it was using BitTorrent client software, UT3420- µTorrent 3.4.2.

c. On April 16, 2015, between the hours of 2:13 a.m. Eastern Daylight Time (EDT) and 4:16 a.m. EDT, a law enforcement computer used and controlled by Investigator Lakatis made a successful connection to a host computer at IP address 66.177.66.109 using an undercover computer through the internet. Using this connection and specialized software, this law enforcement computer successfully downloaded 18 pieces of a total of 30 pieces from the host computer at IP address 66.177.66.109, and through this connection it was confirmed that this host computer possessed 18 of the total of 30 pieces. I know the above information based on conversations with TFO Watson and also from my review of his investigative reports and the disc of downloads from Investigator Lakatis, which were submitted into the FBI's case file management system.

31. On June 3, 2015, TFO Watson conducted a query of Arin, a publicly available online resource, the IP address 66.177.66.109 was determined to be issued to Comcast Communications.



32. On June 4, 2015, TFO Watson prepared an administrative subpoena directed to Comcast Communications requesting the subscriber and billing information for the account associated with IP address 66.177.66.109.

33. On June 5, 2015, the Comcast Legal Response Center responded to this administrative subpoena and provided the subpoena was invalid. TFO Watson was later able to leave Comcast a message, which they responded to June 9, 2015, that the subpoena was invalid due to a typographical error listing the date as 2014 instead of 2015.

34. On June 6, 2015, TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 66.177.66.109 had previously been associated with certain Files of Interest (FOI) by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

35. On June 6, 2015, between the hours of 2:42 a.m. EDT and 3:16 a.m. EDT, TFO Watson, using this connection and specialized software, downloaded from the host computer using IP 66.177.66.109, 29 of the total 599 pieces before the session ended. TFO Watson was also able to confirm that the host computer at IP address 66.177.66.109, possessed 61 of the total of 599 pieces. TFO Watson was able to check the download logs for the partially downloaded video file from IP address 66.177.66.109 entitled, "(pthc) niño se come un pene enorme(2)" and confirmed through several translation sites that this means, "child eats huge penis."

36. On June 6, 2015, between the hours of 2:52 a.m. EDT and 3:16 a.m. EDT, TFO Watson, using this connection and specialized software, downloaded from host computer at IP address 66.177.66.109, 13 of the total 3722 pieces before the session ended. TFO Watson was also able to confirm that the host computer at IP 66.177.66.109 possessed 7 of the total of 3722 pieces at the beginning of the session and 23 of the total 3722 pieces before the session ended. The viewable pieces that were downloaded comprised several different video files. One of the video files contained "PTHC" and "10yo Linda" in the file name and contained at least one child engaged in sexually explicit conduct.

37. On June 10, 2015, TFO Watson prepared a new administrative subpoena directed to Comcast Communications requesting the subscriber and billing information for the account associated with IP address 66.177.66.109 for the date range April 16, 2015, from 2:13 a.m. EDT through 4:16 a.m. EDT and June 6, 2015, from 2:42 a.m. EDT through 3:16 a.m. EDT.

38. On June 11, 2015, TFO Watson received the subpoena response from Comcast Communications. The subscriber information for the IP address 66.177.66.109 during the period between April 16, 2015, from 2:13 a.m. EDT through 4:16 a.m. EDT and June 6, 2015, from 2:42 a.m. EDT through 3:16 a.m. EDT resolved back to the account of Kyle Kirby, 530 Westmoreland Street SE, Live Oak, Florida 32064. The email address associated with this account is [kirbycop@comcast.net](mailto:kirbycop@comcast.net) and service has been provided to this address since October 10, 2012.

39. On June 11, 2015, TFO Watson conducted open source queries, via the Suwannee County Property Appraisers website, and confirmed that the address at 530

Westmoreland Street SE, Live Oak, Florida, 32064, is owned by Kyle Kirby. I conducted a further review of documents and confirmed the sale of the property to Kyle Kirby on April 19, 2011.

40. On June 11, 2015, TFO Watson continued open source queries for Kyle Kirby and located, via Google search, a photograph of an individual named Kyle Kirby in a Live Oak Police Department uniform on the Suwannee High School website, where he was photographed with students. After further records checks, it was determined by TFO Watson that Kyle Kirby was the name of a Live Oak Police Department sergeant.

41. On June 11, 2015, TFO Watson continued open source queries and located a Facebook page depicting the same male identified in the photo above listed under the name Kyle Kirby.

42. On June 12, 2015, I reviewed the Facebook page for Kyle Kirby with TFO Watson and confirmed the Facebook page contained at least one image of Kyle Kirby wearing a Live Oak Police Department Sergeant uniform. I also reviewed the "about" tab on the Facebook page which lists, among other things, Kyle Kirby's "birthday" as September 2, 1980, and "work" as the Live Oak Police Department from September 2, 2003 to present.

43. On June 13, 2015, TFO Watson traveled to Live Oak, Florida to conduct surveillance. TFO Watson went by the residence located at 530 Westmoreland Street SE and checked for open Wi-Fi connections. TFO Watson located one open Wi-Fi for Xfinity, however access required a password for a Comcast account to login. There was a black SUV and a silver Live Oak Police Department patrol car parked in the driveway to the residence. Later this same date, TFO Watson conducted research on

the Comcast website and found they have many locations called Hotspots. Under the FAQ section, TFO Watson found information that stated that although someone may be able to log onto a hotspot, the person logging in and the data they incur will be on their own account, not to the residence or the subscriber at the residence.

44. On July 4, 2015, TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 66.177.66.109 had previously been associated with certain Files of Interest (FOI) by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

45. On July 4, 2015, between the hours of 2:23 a.m. EDT and 2:49 a.m. EDT, TFO Watson, using this connection and specialized software, downloaded from the host computer at IP 66.177.66.109, 142 of the total 599 pieces before the session ended. TFO Watson was also able to confirm that the host computer at IP 66.177.66.109 possessed 599 of the total of 599 pieces. TFO Watson was able to check the download logs for the partially downloaded video file from the host computer at IP address 66.177.66.109 entitled, "(pthc) niño se come un pene enorme (2)" and confirmed again through Google translation that this meant, "(pthc) child a huge penis ( 2) eat."

46. On July 9, 2015, TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 66.177.66.109 had previously been associated with certain Files of Interest (FOI) by investigators conducting keyword searches or info

hash value searches for files related to known child pornography images and videos. Multiple files were acknowledged by the user and included titles and search terms consistent with child sexual exploitation. TFO Watson was not able to view any of the image or videos files in their entirety that were downloaded July 9, 2015, however, was able to review the file directories for the incoming files.

47. On August 7, 2015, TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 66.177.66.109 had previously been associated with certain Files of Interest (FOI) by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

48. On August 7, 2015, between the hours of 2:03 a.m. EDT and 2:04 a.m. EDT, TFO Watson, using this connection and specialized software, downloaded from the host computer at IP address 66.177.66.109, 773 pieces of a total of 773 pieces of an image collection from the host computer at IP address 66.177.66.109, and through this connection it was confirmed that this host computer possessed 773 of the total of 773 pieces.

49. On August 7, 2015, and between 2:13 a.m. EDT and 3:17 a.m. EDT, TFO Watson, using this connection and specialized software, downloaded from host computer at IP address 66.177.66.109, 401 pieces of a total of 3722 pieces. TFO Watson was also able to confirm through this connection that the host computer at IP address 66.177.66.109 possessed 3720 of the total of 3722 pieces.

50. On August 14, 2015, TFO Watson prepared a new administrative subpoena directed to Comcast Communications requesting the subscriber and billing information for the account associated with IP address 66.177.66.109 for the date range April 16, 2015, from 2:13 a.m. EDT through August 7, 2015, 3:17 a.m. EDT.

51. On August 17, 2015, TFO Watson received the subpoena response from Comcast Communications. The subscriber information for the IP address 66.177.66.109 during the period between April 16, 2015, from 2:13 a.m. EDT through August 7, 2015, 3:17 a.m. EDT resolved back to the account of Kyle Kirby, 530 Westmoreland Street SE, Live Oak, Florida 32064. The subpoena result showed that this IP had been leased by the same subscriber since at least February 15, 2015. Comcast only retains subscriber IP information for 180 days. TFO Watson also spoke with a Comcast representative in the legal department on a separate case and confirmed that if this IP address was connected as a Wi-Fi hotspot it would show the subscriber's data who connected and not the subscriber data from the physical location.

52. On September 12, 2015, TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 73.148.219.91 had previously been associated with certain Files of Interest (FOI) by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

53. On September 12, 2015, between the hours of 12:12 a.m. EDT and 12:48 a.m. EDT, TFO Watson, using this connection and specialized software, downloaded

from the host computer at IP 73.148.219.91, 202 of the total 217 pieces before the session ended.

54. On October 7, 2015, TFO Watson prepared a new administrative subpoena directed to Comcast Communications requesting the subscriber and billing information for the account associated with IP address 73.148.219.91 for the date range September 12, 2015, from 12:12 a.m. EDT through September 12, 2015, 12:48 a.m. EDT.

55. On October 8, 2015, TFO Watson received the subpoena response from Comcast Communications. The subscriber information for the IP address 73.148.219.91 for the date range September 12, 2015, from 12:12 a.m. EDT through September 12, 2015, 12:48 a.m. EDT resolved back to the account of Kyle Kirby, 530 Westmoreland Street SE, Live Oak, Florida 32064.

56. Subsequently, I reviewed the image files that Investigator Lakatis caused to be downloaded from the host computer connected to the Internet through IP address 66.177.66.109 on April 16, 2015. Based on my training and experience, I believe that several of the image files depict at least one minor engaged in sexually explicit conduct, and therefore constitute child pornography pursuant to Title 18, United States Code, Section 2256. As described herein, the SHA-1 values for several of these images are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). Two of the images that Investigator Lakatis caused to be downloaded from IP address 66.177.66.109 on April 16, 2015, between the hours 2:13

a.m. EDT and 4:16 a.m. EDT, that were being offered for sharing on the date and times listed below, are described as follows:

SHA-1: OIT2EJU6BWXE2GI36ZTR3M7UVRKLX6HN

DATE: April 16, 2015, between the hours 2:13 a.m. EDT and 4:16 a.m. EDT

TITLE: 000005.jpg

DESCRIPTION: This is a color still image which depicts two prepubescent children. The children are fully nude lying in the grass, with one child lying down and the other child straddling the first child. It is difficult to determine whether the child lying down is male or female due to poor quality of the photo. The child on top appears to be a female around 9-10 years old. The position of the children in the photo, as well as the nudity, is consistent with a sexual act.

SHA-1: 4DLEZGX35LY7A7BXS4VCL4TGLTKE5AYF

DATE: April 16, 2015, between the hours 2:13 a.m. EDT and 4:16 a.m. EDT

TITLE: 000006.jpg

DESCRIPTION: This is a color still image which depicts a prepubescent female. The child is wearing a white dress with no underwear. Her right leg is curled beneath her and her left leg is lifted up. The child's vagina is clearly visible and appears to be the focal point of the photo; it is close to center of the photograph and is in focus.

57. Subsequently, I reviewed the image files that TFO Watson caused to be downloaded from the host computer connected to the Internet through IP address 66.177.66.109 on June 6, 2015. Based on my training and experience, I believe that several of the video files depict at least one minor engaged in sexually explicit conduct, and therefore constitute child pornography pursuant to Title 18, United States Code,



Section 2256. As described herein, the SHA-1 values for several of these files are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). Two of the files that TFO Watson caused to be downloaded from IP address 66.177.66.109 on June 6, 2015, between the hours 2:42 a.m. EDT and 3:01 a.m. EDT, that were being offered for sharing on the date and times listed below, are described as follows:

SHA-1: fd51224dd9eca7b12cca4f32b0aa5009308a0653

DATE: June 6, 2015, between the hours 2:42 a.m. EDT and 3:01 a.m. EDT

TITLE: (pthc) niño se come un pene enorme(2).mpg

DESCRIPTION: This is a partial download of a color video without audio approximately 00:19 (minutes:seconds) in length. The video begins with an adult male seated in a chair with a fully clothed child seated on his lap. The video skips and the prepubescent male child's pants have been pulled down and the adult male is masturbating the child. The video then skips and depicts an adult male inserting his penis into the anus of a prepubescent male child. The sexual explicit conduct continues until the video terminates.

SHA-1: 519def775a39427eb53381b4735679391a343c14

DATE: June 6, 2015, between the hours 2:52 a.m. EDT and 3:01 a.m. EDT

TITLE: T-101924864-(Pthc) 10Yo Linda – Dando A Bucetinha Pro Papai Pedo Ptsc Hussyfan Lolita.avi

DESCRIPTION: This is a partial download of a color video without audio approximately 01:44 (minutes:seconds) in length. The video depicts a prepubescent

female child wearing a black concealing garment over her head, climbing atop a nude adult male. The video freezes until the closing frames, where the child is seen straddling the nude adult male.

58. Subsequently, I reviewed the files that TFO Watson caused to be downloaded from the host computer connected to the Internet through IP address 66.177.66.109 on August 7, 2015 between the hours of 2:13 a.m. EDT on August 7, 2015, and 2:55 a.m. EDT on August 7, 2015. Based on my training and experience, I believe that at least one of the video files depict at least one minor engaged in sexually explicit conduct, and therefore constitute child pornography pursuant to Title 18, United States Code, Section 2256. As described herein, the SHA-1 values for these files are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). Two of the files that TFO Watson caused to be downloaded from IP address 66.177.66.109 on August 7, 2015 between the hours of 2:13 a.m. EDT on August 7, 2015, and 2:55 a.m. EDT, that were being offered for sharing on the date and times listed below, are described as follows:

SHA-1: 9349bcfd0d807e88802abb4b14fe4880701fbcf1

DATE: August 7, 2015, between the hours 2:13 a.m. EDT and 2:55 a.m. EDT

TITLE: 3.mpg

DESCRIPTION: This is a color video without audio approximately 06:01 (minutes:seconds) in length depicting a female child with no indications of puberty. The child does not show any evidence of pubic hair or breast development. The video begins with the child seated on a bed. The child is wearing black stockings and a white

nightgown. The child then rolls over on her stomach and the cameras zooms in to show her spreading her buttocks with her hands. She rolls back over onto her back and the camera zooms in to show her spreading her vaginal opening with her hands. The camera zooms back out and the child removes the nightgown, showing her undeveloped breasts. She massages her right breast with her right hand and the camera zooms in close on this as well. The video continues as the girl makes various poses on the bed. The child at one point bends over backward with her hands and feet on the bed and her back arched; the camera again zooms in on her vaginal area. The child can be seen looking at the camera and it appears that she is taking direction. The child reaches into a dresser drawer next to the bed and retrieves an off white colored sexual device that is penile shaped. The remainder of the video zooms in and out several times as the child rubs the device against her vagina. The video ends with a close up of the girl's vagina while she is lying on the bed.

SHA-1: 519def775a39427eb53381b4735679391a343c14

DATE: August 7, 2015, between the hours 2:13 a.m. EDT and 2:55 a.m. EDT

TITLE: T-101924864-(Pthc) 10Yo Linda – Dando A Bucetinha Pro Papai Pedo  
Ptsc Hussyfan Lolita.avi

DESCRIPTION: This is a color video without audio approximately 01:43

(minutes:seconds) in length which depicts a prepubescent female child wearing a black concealing garment over her head, climbing atop a nude adult male. The child sits on the adult male facing away, and his penis is inserted in the child's vagina. The child moves up and down on the adult male's penis until approximately 00:54 of the video,

when she moves and faces the adult man, inserting his penis into her vagina. This sexual explicit conduct continues until the video terminates.

59. I made an investigative decision not to conduct a query of the Florida Drivers and Vehicle Information Database (DAVID) for persons holding a State of Florida Driver's License or Identification Card residing at 530 Westmoreland Street SE, Live Oak, Florida, 32064. This was based solely on the fact law enforcement officers residing in Florida receive notification of queries and the agency running the query.

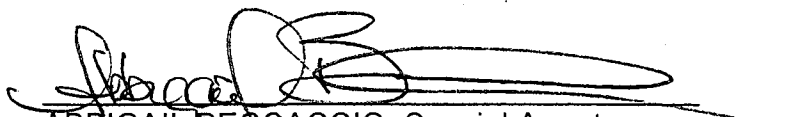
60. At my request, on October 15, 2015, TFO Watson traveled to Live Oak, Florida to conduct surveillance. TFO Watson went by the residence located at 530 Westmoreland Street SE, Live Oak, Florida, 32064. There was a dark colored Chevy SUV and a silver Live Oak Police patrol car parked in the driveway to the residence. The car had "police" on the side but did not have overhead lights.

### **CONCLUSION**

61. Based on the foregoing, I have probable cause to believe that one or more individuals has used and is using one or more computers and/or electronic storage media located in the residence located at 530 Westmoreland Street SE, Live Oak, Florida, 32064, more fully described in Attachment A to this affidavit, to, among other things, receive and possess child pornography. Therefore, I have probable cause to believe that one or more individuals, using the residence described above has violated 18 U.S.C. §§ 2252 and 2252A. Additionally, I have probable cause to believe that fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including at least one computer and other electronic storage media containing images of child

pornography, and the items more fully described in Attachment B to this affidavit (which is incorporated by reference herein), will be located in this residence.

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

  
ABBIGAIL BECCACCIO, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this  
21<sup>st</sup> day of October, 2015, at Jacksonville, Florida.

  
MONTE C. RICHARDSON  
United States Magistrate Judge

## ATTACHMENT A

### PREMISES TO BE SEARCHED

The residence located at 530 Westmoreland Street SE, Live Oak, Florida, 32064, is a single story, residential home with a yard enclosed by a wooden privacy fence. The home's exterior is tan in color with grey decorative shutters, and a tan colored roof. There is a small covered front porch on the front of the residence facing the road with a waist-high white picketed railing. The front yard features several leafy trees and bushes and includes a lamp post which is overgrown with vine. To the right of the front door (when facing the residence from Westmoreland Street SE) are two windows, with grey shutters. To the left of the front door from this same vantage point are two additional windows with grey shutters. Continuing in this direction is what appears to be a Florida room that has been converted from a garage. This room has grey awnings over the windows. There is an American flag on the northeast corner of this room and below the windows with the awning is an FSU lawn flag. There is a sidewalk that leads to the front porch from Westmoreland Street SE. The driveway and parking area are paved with black asphalt. The asphalt goes around a split trunk oak tree. There is a flag beneath this tree with a K on it. There is a black mailbox that bears the numerals "530" near the large oak tree.

## ATTACHMENT B

### LIST OF ITEMS TO BE SEIZED AND SEARCHED

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

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

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession,

receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or referencing and/or discussing sexual activity involving minor children.

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

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

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

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in



18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

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

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online

storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

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

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

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

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

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

# UNITED STATES DISTRICT COURT

for the  
Middle District of Florida

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )

a residence located at 530 Westmoreland Street SE )  
Live Oak, Florida, 32064, more particularly )  
described in Attachment A )

Case No. 3:15-mj-1210-MCR

## 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):

A residence located at 530 Westmoreland Street SE, Live Oak, Florida, 32064, more particularly decribed in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):  
See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before

11/1/15

(not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m.

at any time in the day or night as I find reasonable 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 United States Magistrate Judge Monte C. Richardson

(name)

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:

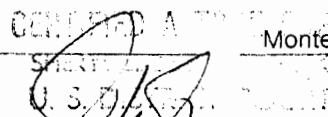
10/21/15 @ 4:19 a.m.

Monte C. Richardson  
Judge's signature

City and state: Jacksonville, Florida

Monte C. Richardson, United States Magistrate Judge

Printed name and title



By: \_\_\_\_\_

Deputy Clerk

## ATTACHMENT A

### PREMISES TO BE SEARCHED

The residence located at 530 Westmoreland Street SE, Live Oak, Florida, 32064, is a single story, residential home with a yard enclosed by a wooden privacy fence. The home's exterior is tan in color with grey decorative shutters, and a tan colored roof. There is a small covered front porch on the front of the residence facing the road with a waist-high white picketed railing. The front yard features several leafy trees and bushes and includes a lamp post which is overgrown with vine. To the right of the front door (when facing the residence from Westmoreland Street SE) are two windows, with grey shutters. To the left of the front door from this same vantage point are two additional windows with grey shutters. Continuing in this direction is what appears to be a Florida room that has been converted from a garage. This room has grey awnings over the windows. There is an American flag on the northeast corner of this room and below the windows with the awning is an FSU lawn flag. There is a sidewalk that leads to the front porch from Westmoreland Street SE. The driveway and parking area are paved with black asphalt. The asphalt goes around a split trunk oak tree. There is a flag beneath this tree with a K on it. There is a black mailbox that bears the numerals "530" near the large oak tree.

## ATTACHMENT B

### LIST OF ITEMS TO BE SEIZED AND SEARCHED

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

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

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession,

receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or referencing and/or discussing sexual activity involving minor children.

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

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

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

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in

18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

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

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online



storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

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

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

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

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

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