

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America

v.

MICHAEL EUGENE WILLIAMS

Defendant(s)

Case No.

3:16-mj-1278-MCR

FILED IN OPEN COURT

10.21.16

CLERK, U.S. DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE, FLORIDA

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 March 9, Sept. 28 & Oct. 21, 2016, in the county of Duval in the
Middle District of Florida, the defendant(s) violated:*Code Section**Offense Description*

18 U.S.C. § 2251(d)(1)(A)

Publishing a notice seeking a visual depiction of a minor engaging in sexually explicit conduct

18 U.S.C. § 2252(a)(2)

Receipt of a visual depiction the production of which involved the use of a minor engaging in sexually explicit conduct

18 U.S.C. § 2252(a)(4)

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

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.*Complainant's signature*

Anthony Algozzini, HSI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

10/21/16*Judge's signature*

City and state:

Jacksonville, Florida

Monte C. Richardson, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Anthony Algozzini, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent with U.S. Immigration and Customs Enforcement (ICE) / Homeland Security Investigations (HSI), an agency of the United States Department of Homeland Security (DHS). I have been employed since May of 2003 and I am currently assigned to the Office of the Assistant Special Agent in Charge, Jacksonville, Florida. I have successfully completed the Criminal Investigator Training Program and ICE Special Agent Training Academy at the Federal Law Enforcement Training Center in Brunswick, Georgia. I am classified and trained as a Federal Law Enforcement Officer, with federal statutory arrest authority. In my capacity as a Special Agent, I have participated in numerous types of criminal investigations, during the course of which I have conducted or participated in physical surveillance, undercover transactions, executions of search and arrest warrants, controlled delivery transactions of narcotics and other contraband, asset forfeiture including real property, and other complex investigations. I hold a Bachelor of Science degree in International Business from the College of Charleston. I have attended advanced training in criminal investigations including training regarding the investigation of Internet crimes against children and computer crimes. Internet Crimes Against Children (ICAC) is a national organization which provides

specialized high-technology training and resources to law enforcement agencies that investigate crimes dealing with the online sexual solicitation and sexual exploitation of children, including the collection and trading of images of child pornography. The following is a list of courses in which I have received training: ICAC CyberTips Overview, ICAC Peer to Peer Essentials, and ICAC Ares Investigations (dealing specifically with the investigation of child pornography distribution through the use of peer-to-peer computer networks). I have an understanding of the Internet and have conducted and participated in investigations involving the production, receipt, transportation, distribution, and possession of child pornography.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of Title 18, United States Code, Sections 2252 and 2252A, as well as Florida state statutes that 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 establishing probable cause for the filing of a criminal complaint, and I have not included each

and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that MICHAEL EUGENE WILLIAMS has committed violations of Title 18, United States Code, Sections 2251(d)(1)(A) (Publishing a notice seeking a visual depiction of a minor engaging in sexually explicit conduct); 2252(a)(2) (Receipt of a visual depiction the production of which involved the use of a minor engaging in sexually explicit conduct); and 2252(a)(4) (Possession of a visual depiction the production of which involved the use of a minor engaging in sexually explicit conduct), is present in the premises and items to be searched.

4. This affidavit is made in support of a complaint against MICHAEL EUGENE WILLIAMS, that is, on or about March 9, 2016, in Duval County, in the Middle District of Florida and elsewhere, MICHAEL EUGENE WILLIAMS did, using a facility and means of interstate and foreign commerce, knowingly make, print and publish, and cause to be made, printed and published, a notice and advertisement seeking and offering to receive a visual depiction, the production of which visual depiction involves the use of a minor engaging in sexually explicit conduct and which depiction is of such conduct, in violation of Title 18, United States Code, Section 2251(d)(1)(A); on or about September 28, 2016, did receive a visual depiction, the production of which involved the use of a minor engaging in sexually explicit conduct and which depiction was of such conduct and, on or about

October 21, 2016, did possess depictions involving the use of a minor engaging in sexually explicit conduct, which visual depictions have actually been transported and transmitted using a means and facility of interstate commerce, that is, via the Internet, in violation of Title 18, United States Code, Section 2252(a)(4).

5. On October 20, 2016, I applied for and obtained a federal search warrant for the premises located at 8985 Normandy Blvd., Lot 62, Jacksonville, Florida, 32221, which I believed to be occupied by MICHAEL EUGENE WILLIAMS, a copy of which is attached hereto as Exhibit A, and the facts and information contained therein are hereby incorporated by reference.

6. On October 21, 2016, HSI – Jacksonville special agents, along with Jacksonville Sheriff's Office officers, executed the aforementioned search warrant at approximately 7:00 a.m. I observed MICHAEL EUGENE WILLIAMS exit the premises upon instruction by law enforcement to do so. Upon search of the subject premises, I observed an LG cellular telephone, Model No. LG-H631, on the nightstand of a bedroom (the "LG telephone"). The LG telephone had a stamp, "Made in China."

7. A preliminary examination of the LG telephone conducted on scene during the execution of the search warrant revealed videos of child pornography. I reviewed two such videos and, based on my training and experience, I believe the

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.

TITLE: 4237c0dd-37f4-458c-8c44-48a0ac98dfa7.mp4

DESCRIPTION: This file is an 18-second video depicting a young pre-pubescent female child, who appears to be standing on a bed, positioned in front of the camera, bent over at the waist displaying her genitalia, which is the focal point of the video. The minor child is seen moving her buttocks back and forth while continuing to display her genitalia. The child's face is not visible.

8. Another video discovered through the preliminary on-scene examination of the LG telephone was transmitted to the LG telephone via the Kik Messaging application, which was installed on the LG telephone. I reviewed chat messages that appeared to take place between Kik user Linzi_██████████²⁴¹ and a Kik user of the LG telephone. Specifically, I discovered communication taking place on September 28, 2016, through which a video was sent by Linzi_██████████²⁴ to the LG telephone. I reviewed the video and, based on my training and experience, I believe the video depicts at least one minor engaged in sexually explicit conduct, and

¹ As mentioned in Exhibit A, I have redacted the user name to protect the identity of the minor victim given the familial relationship between the minor victim and an individual I believe to be Linzi S.

therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

FROM: Linzi_██████████24
TO: LG telephone
TIMESTAMP: September 28, 2016 4:33:02 PM (UTC)
TITLE: 072e0981-60f7-4a1a-abbd-30b1146cb1a8.mp4

DESCRIPTION: The file is a 4-second video depicting a young pre-pubescent female child, who appears to be nude and can be seen from the chest down, laying on her back with her legs spread apart, displaying her genitalia with her knees pulled up on either side of her. Her left arm is across her upper torso and her right hand is holding what appears to be a purple popsicle, rubbing the popsicle over her bare genitalia. The pre-pubescent female child's vagina is within view and the focal point of the video.

9. After receipt of the above-described video, the LG telephone sent the following response message to Linzi_██████████24:

LG telephone: *Mmmmmmm I love grape can I lick it off?*
Linzi_██████████24: *It's multi flavor.*
LG telephone: *Can I lick it? It looks so wet and juicy.*
Linzi_██████████24: *That guarantees me the money.*
LG telephone: *Yeah baby.....you got Daddy jerking off now....can you get a longer video of her?*

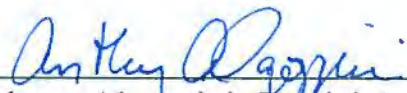
10. During the execution of the search warrant, I also encountered Nam Sun Durby a/k/a Sandra Durby, who also resided in the home with MICHAEL EUGENE WILLIAMS. Jacksonville Sheriff's Office Detective Jessica Maynard told me that she interviewed Durby, who advised that the LG telephone belonged to MICHAEL EUGENE WILLIAMS, and that WILLIAMS acquired the telephone shortly after the execution of the previous search warrant at the residence. Durby further advised Detective Maynard that she did not know the password to access the LG telephone and had never used it before.

11. Also found during the execution of the search warrant were Western Union receipts showing money wire transfers from MICHAEL WILLIAMS to Bobby S [REDACTED], who I believe to be the husband of Linzi S [REDACTED], in the amount of \$40 each with one showing a transaction occurring on August 29, 2016 and another occurring on September 8, 2016.

CONCLUSION

12. Based upon the foregoing facts, and including those facts set forth in Exhibit A, I have probable cause to believe that on or about March 9, 2016, MICHAEL EUGENE WILLIAMS did, using a facility and means of interstate and foreign commerce, knowingly make, print and publish, and cause to be made, printed and published, a notice and advertisement seeking and offering to receive a visual depiction, the production of which visual depiction involves the use of a minor

engaging in sexually explicit conduct and which depiction is of such conduct, in violation of Title 18, United States Code, Section 2251(d)(1)(A); on or about September 28, 2016, did receive a visual depiction, the production of which involved the use of a minor engaging in sexually explicit conduct and which depiction was of such conduct and, on or about October 21, 2016, did possess depictions involving the use of a minor engaging in sexually explicit conduct, which visual depictions have actually been transported and transmitted using a means and facility of interstate commerce, that is, via the Internet, in violation of Title 18, United States Code, Section 2252(a)(4).



Anthony Algozzini, Special Agent
Homeland Security Investigations- Jacksonville

Sworn to before me this
this 21st day of October, 2016



MONTE C. RICHARDSON
United States Magistrate Judge

EXHIBIT A

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)*premises located at 8985 Normandy Blvd., Lot 62,
Jacksonville, FL 32221,
described further in Attachment A

Case No. 3:16-mj- 1277-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)*:

premises located at 8985 Normandy Blvd., Lot 62, Jacksonville, FL 32221, described further in Attachment A,
located in the Middle District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

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

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

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252	Receipt, distribution and possession of material involving the sexual exploitation of a minor
18 U.S.C. § 2252A	Receipt, distribution and possession of material containing 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.



Applicant's signature

Anthony Algozzini, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

10/20/16

CERTIFIED A TRUE COPY

SHERYL L LOESCH, CLERK

U.S. DISTRICT COURT

By:

Deputy Clerk


Judge's signature

MONTE C. RICHARDSON, U.S. Magistrate Judge

Printed name and title

City and state: Jacksonville, Florida

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is a residence located at 8985 Normandy Boulevard Lot 62, Jacksonville, FL 32221, identified as a single story double wide mobile home that is gray in color. The first floor primarily consists of gray painted siding. There is a concrete driveway to the residence which is positioned at an angle on the lot. There are six steps facing south that lead up to a gate before accessing a covered front porch to access the front door facing west. The numbers "62" are visible on the south and west corners of the residence. The residences on either side near the premises are single wide mobile homes. The back door is on the east side of the residence at the north side of the trailer with a small wood porch. The back yard has a wood privacy fence to the north separating the mobile home park from the adjoining neighborhood but no fences are present between each mobile home. There are no other residences in the immediate area that look the same.

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, personal digital assistants (PDA), digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images), computer-related documentation, computer passwords and data-security devices, videotapes, video recording devices, video recording players, and video display monitors that are or may be used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography or child erotica.

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

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs

and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

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

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

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

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and

electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

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

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

12. Any and all cameras, film, videotapes or other photographic equipment that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the

United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Anthony Algozzini, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent with U.S. Immigration and Customs Enforcement (ICE) / Homeland Security Investigations (HSI), an agency of the United States Department of Homeland Security (DHS). I have been employed since May of 2003 and I am currently assigned to the Office of the Assistant Special Agent in Charge, Jacksonville, Florida. I have successfully completed the Criminal Investigator Training Program and ICE Special Agent Training Academy at the Federal Law Enforcement Training Center in Brunswick, Georgia. I am classified and trained as a Federal Law Enforcement Officer, with federal statutory arrest authority. In my capacity as a Special Agent, I have participated in numerous types of criminal investigations, during the course of which I have conducted or participated in physical surveillance, undercover transactions, executions of search and arrest warrants, controlled delivery transactions of narcotics and other contraband, asset forfeiture including real property, and other complex investigations. I hold a Bachelor of Science degree in International Business from the College of Charleston. I have attended advanced training in criminal investigations including training regarding the investigation of Internet crimes against children and computer crimes. Internet Crimes Against Children (ICAC) is a national organization which provides specialized high-technology training and resources to law enforcement agencies that investigate crimes dealing with the online sexual solicitation and sexual exploitation

of children, including the collection and trading of images of child pornography. The following is a list of courses in which I have received training: ICAC CyberTips Overview, ICAC Peer to Peer Essentials, and ICAC Ares Investigations (dealing specifically with the investigation of child pornography distribution through the use of peer-to-peer computer networks). I have an understanding of the Internet and have conducted and participated in investigations involving the production, receipt, transportation, distribution, and possession of child pornography.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of Title 18, United States Code, Sections 2252 and 2252A, as well as Florida state statutes that 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 premises 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, or other materials that contain 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.

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

b. "Child pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involves the use of a minor engaging 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 engaging in sexually explicit conduct, or (c) the visual depiction has been created,

adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct).

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

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

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

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external

hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

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

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data

files and printouts or readouts from any magnetic, electrical or electronic storage device).

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

k. "Wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio

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

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

m. A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

n. A personal digital assistant, or “PDA,” is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

o. A “tablet” is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “Wi-Fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

p. A “pager” is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

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 a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs

themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

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

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, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding 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 millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown

tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

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

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

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

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system, which includes the use of data search protocols, is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

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 in the area of investigating cases involving the sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

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

b. Many individuals who collect child pornography collect 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 rise to the level 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 and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P) file-sharing programs, 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. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, 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, I learned of an investigation in 2007 in the Middle District of Florida from FBI SA Lawrence S. Meyer in which 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.

16. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collection of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures; may 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 may send it to third party image storage sites via the Internet.

KIK MESSENGER APPLICATION

17. Through my research, investigations involving the Kik Messenger Application and from information obtained from other law enforcement officers, I know the Kik Messenger application is primarily a social media mobile device platform designed and managed by Kik Interactive Incorporated, a Waterloo, Canada-based company, for the purpose of mobile messaging and communication. To use this application, a user downloads the mobile messaging application via an applications service such as the Google Play Store, Apple iTunes, or other similar mobile application provider. Once downloaded and installed, the user is prompted to create an account and a username. This username will be the primary account identifier. The user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik users are asked to supply a valid email address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by other users. Once the Kik user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between the two parties.

18. Kik Messenger also allows users to create chat rooms, of up to 50 people, for the purpose of communicating and exchanging images and videos. These rooms are administered by the creator who has the authority to ban and remove

other users from the created room. According to Kik Messenger, more than 40% of the Kik users chat in “groups” and approximately 300,000 new groups are created every day. These groups are frequently created with a “hashtag” allowing the group or chat to be identified more easily. Once the group or chat is created, Kik users have the option of sharing the “link” with all of their contacts or anyone they wish.

19. Kik Messenger users frequently advertise their Kik usernames on various social networking sites in order to meet and connect with other users. In some cases, Kik also provides various avenues, such as dating sites and social media applications, for meeting other users. I know from various HSI undercover investigations, many Kik users have stated they felt safe using Kik Messenger as a means of trading child pornography and for other illegal activities because “Kik is a Canadian based company and not subject to the same United States laws.” HSI undercover agents have noted messages posted in Kik Messenger chat rooms discussing Kik’s enforcement, deletion, or banning of users and rooms used for the purpose of exchanging or distributing child pornography. HSI agents also have noted the comments to include the continued creation of new rooms and new user accounts to attempt to circumvent Kik Messenger’s enforcement efforts.

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

20. I make this affidavit in support of a search warrant for the premises located at 8985 Normandy Boulevard Lot 62, Jacksonville, FL 32221 (the “Subject Premises”), which I believe to be currently occupied by Michael Eugene Williams

(date of birth January 28, 1957). I have personally observed the Subject Premises, and it appears as set forth in Attachment A. Digital photographs of the Subject Premises were taken on October 20, 2016, and the photographs are consistent with the description as set forth in Attachment A.

21. HSI-Jacksonville and the Jacksonville Sheriff's Office is investigating the use of one or more computers and computer media at the Subject Premises 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.

22. On October 5, 2016, I spoke with Detective Jessica Maynard with the Jacksonville Sheriff's Office regarding this investigation and the facts establishing probable cause. Jessica Maynard is a Detective for the Jacksonville Sheriff's Office with over fifteen (15) years of law enforcement experience. Detective Maynard is currently assigned to the ICAC Task Force. Prior to this assignment, Detective Maynard was assigned as a Detective in the Special Assault Unit of the Jacksonville Sheriff's Office specializing in Sex Crimes and Child Abuse Investigations for approximately 5 years. Detective Maynard's duties include taking an active role in criminal investigations that relate to the online exploitation of children. Detective Maynard has received specialized training through the United States Department of Justice, Office of Juvenile and Delinquency Prevention related to Internet Crimes Against Children Investigative Techniques, Undercover Chat Operations, and various

Peer to Peer (P2P) programs. Detective Maynard is a member of the North Florida ICAC Task Force. ICAC is a national organization which provides specialized high-technology training and resources to law enforcement agencies that investigate crimes dealing with online sexual-solicitation and sexual-exploitation of children, including the collection and trading of images of child pornography. Detective Maynard has an understanding of the Internet and has participated in investigations involving undercover chat sessions, child sexual-solicitation, and the receipt, transportation, distribution and possession of child pornography. Detective Maynard has also attended several advanced trainings in Sex Crimes Investigations, Sex Trafficking Investigations, Child Abuse/Neglect Investigations, and Deviant Sexual Behavior Investigations. Detective Maynard has investigated and/or assisted in investigations of crimes against children including: Child Neglect, Physical Child Abuse, Sexual Child Abuse, Online Enticement of Children, Obscenity Directed at Minors, and Travelling with the Intent to have Sex with Minors. Detective Maynard has investigated and/or assisted in the investigation of matters involving the possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography. Detective Maynard has 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.

23. On October 5, 2016, Detective Maynard told me:

a. On May 26, 2016, Detective Maynard received a Cyber Tip from the National Center for Missing and Exploited Children (NCMEC; Tip #11561767). The Cyber Tip originated from Legal Compliance personnel from Google, Inc., who reported that they had discovered what was believed to be child pornography files uploaded from Internet Protocol ("IP") address 108.200.194.134 and Internet Protocol ("IP") address 2607:tb90:4092:fe1:622d:2a87:975c:eac7 to a Google Drive account. Google Drive is a file storage synchronization service created by Google, Inc., which allows users to store and/or share files, to include both videos and photos, in their drive. These items are then automatically saved to the Google Drive website as well as to the user's computers and phones that accessed the images. Detective Maynard viewed the reported files and determined, based on her training and experience, that the files are child pornography images and videos. Google, Inc. personnel also reported that the user/subscriber of this particular Google Drive account had an associated e-mail address of "michaelredeemed@gmail.com" and an associated phone number of "904-729-6485." The aforementioned email address and phone number was used by the user/subscriber when creating the Google Drive account. There were eleven (11) files provided within the Cyber Tip. Detective Maynard personally viewed the eleven (11) files and determined that six (6) of them were in fact child pornography photographs and five (5) were child pornography videos. Based on Detective Maynard's training and experience, she believes each of the files depicts at least one prepubescent child engaged in sexually explicit conduct. The six (6) child pornography pictures were uploaded to the Google Drive account

from the Internet Protocol ("IP") address 2607:fb90:4092:f7e1:622d:2a87:975c:eac7 and the five (5) child pornography videos were uploaded from Internet Protocol ("IP") address 108.200.194.134.

I reviewed the files Detective Maynard Craven advised were uploaded to the above mentioned Google Drive. Based on my training and experience, I believe the files depicts at least one minor engaged in sexually explicit conduct, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256. Described below are the three of the files that Detective Maynard advised were uploaded to the Google Drive account from the above mentioned IP Addresses:

DATE: 05-08-2016 14:26:12 UTC

TITLE: oio5777.mp4

IP ADDRESS: 108.200.194.134

DESCRIPTION: This file was a color video thirty-six (36) seconds in length that displayed a young, apparently naked, pre-pubescent female child. The video begins in the middle of penile vaginal intercourse zoomed in to the genitalia of the child. The child is lying on her back and appears to be on top of a linen or bedspread that is light multi-colored. An adult hand is visible in the left of the screen, holding the child's right leg up. At approximately five (5) seconds, the adult hand utilizes the thumb to molest and push on the child's genitalia while continuing penile penetration of the child's vagina. At approximately eight (8) seconds, the hand is removed from the child's genitalia and placed on the penis at approximately eleven (11) seconds as penile thrusting into the child's vagina continues. At approximately fourteen (14)

seconds, the adult hand continues to hold the penis as he ejaculates onto the child's stomach as the video pans out slightly. The hand rubs the tip of the penis against the child's vagina as he continues to ejaculate. At approximately twenty-one (21) seconds, the child's hands become visible and the child's right hand touches the semen and rubs it around her genitalia. At approximately twenty-seven (27) seconds, the adult penis penetrates the young child's vagina as the video pans slightly in and out and then cuts off. The video of the young pre-pubescent female child's vagina being penetrated by an adult penis until ejaculation are within view and the focal point of the image.

DATE: 05-08-2016 15:16:28 UTC

TITLE: c73a1e2b-16c3-4e6e-b31d-92e120ffca13.webm

IP ADDRESS: 108.200.194.134

DESCRIPTION: This file was a color video two (2) minutes and twenty-five (25) seconds in length which began by displaying a still picture of a young naked pre-pubescent female child. The small child is on her knees, bending over with her buttocks raised and her head and arms lowered. The image was taken from a first person position directly behind and above the child as she's being anally penetrated by an adult penis. The image of the very young pre-pubescent female child's anus being penetrated by an adult penis is within view and the focal point of the image. At approximately ten (10) seconds, the video changes to a very young pre-pubescent female child of similar size and stature of the image previously displayed, being anally penetrated by an adult penis. The child is again on her knees, facing

downward with her buttocks raised as she is being deeply penetrated anally by an adult penis. The child is apparently naked from the waist down and has what appears to be a light pink dress with flowers pushed up around her torso. The child is lying on what appears to be a white linen sheet or bedspread. The camera angle is above the child yet from the side showing the child to the left and the adult penis to the right of the screen. Based on the movement of the camera and approximate arm length distance away, the video gives the appearance of being recorded by the male that is sexually battering the child. At approximately fourteen (14) seconds, the camera pans out slightly to show the small child's entire body as the light brown haired child is laying her head on her crossed arms while lying face down with her head turned to the side and her hair covering her face. Based on the overall diminutive size of the child, compared to the adult's penis and legs, the child appears to be approximately 2-6 years of age. At approximately one (1) minute and twenty-one (21) seconds, the camera pans in for a closer view of the adult penis penetrating the small child's anus. The penis is continually thrusting into the small child's anus until, at approximately one (1) minute and forty-three (43) seconds, the penis comes out the child's anus and the man's right hand assists in reinserting the penis back into the child's anus. At approximately two (2) minutes and thirteen (13) seconds, the video fades to black and then a still image appears for the remainder of the video.

DATE: 03-24-2016 19:52:19 UTC

TITLE: IMAG0141.jpg

IP ADDRESS: 2607:fb90:4092:f7e1:622d:2a87:975c:eac7

DESCRIPTION: The still image is an image at close range of a very young prepubescent female child's genitalia. The child's legs are spread open to display her vagina and anus as an adult hand is using the thumb and forefinger to spread the anus gaping open. The image of the very young pre-pubescent female child's vagina and anus being digitally spread open by an adult hand is within view and the focal point of the image. The child is lying on her back with an adult hand molesting the child's genitalia.

b. On May 27, 2016, Detective Maynard received a Cyber Tip from the National Center for Missing and Exploited Children (NCMEC; Tip #11850960). The Cyber Tip originated from Legal Compliance personnel from Google, Inc., who reported that they had discovered an email thread indicating the subject may have abused a friend or relative's child and is trading child pornography. The Google email thread correspondence involved michaelredeemed@gmail.com

c. Detective Maynard conducted an internet search on the origin of IP Address 108.200.194.134 and determined that the IP Address resolved to AT&T Internet Services.

d. On May 27, 2016, Detective Maynard caused a subpoena to be served to AT&T Internet Services, requesting all available account subscriber information for IP address 108.200.194.134. Detective Maynard told me about the responsive documents received by Detective Maynard on May 27th, 2016, which disclosed the following information about the subscriber for IP address 108.200.194.134:

Subscriber Name: Sandra Durby

Service Address: 8985 Normandy Blvd, Lot 62

Jacksonville, FL 32221

Telephone #: 904-405-3026

Type of Service: High Speed Internet Service

Account Number: 132708750

IP Assignment:

MAC Address:

Dynamically Assigned

28: 16:2e:e3 :20:98

E-mail User Ids: kimdurby@att.net

sandradurby@gmail.com

Method of Payment: Paperless Billing address of

213 Crosswinds Chesapeake, VA 23320

e. Detective Maynard told me that the six (6) images uploaded from the Internet Protocol ("IP") address 2607:fb90:4092:f7e1:622d:2a87:975c:eac7 are all involving the same very young white female child. The focal point of all six (6) images is the child's genitalia to include three (3) of the images showing the adult hand molesting the child's vagina and one (1) image of the child's legs spread wide open. In the six (6) images, the child is laying on her back on a multi-colored, multi-patterned fabric that appears to be a possible bedspread, quilt or comforter. The images show what appears to be a

mole to the right side of the child's vagina and what appears to be a possible scar on the child's left ribcage area.

f. Detective Maynard told me that NCMEC Cyber Tip 11561767 specifically Note #5, which I reviewed, states that "EXIF information for 6 of the images (IMAG0140.jpg, IMAG0141.jpg, IMAG0143.jpg, IMAG0144.jpg, IMAG0145.jpg and IMAG0146.jpg) reveal that they were captured within approximately one hour of being uploaded via a cellular device (T-Mobile USA)."

g. Detective Maynard conducted an internet search on the origin of IP Address 2607:fb90:4092:f7e1:622d:2a87:975c:eac7 and determined that the IP Address resolved to T-Mobile.

h. On May 27, 2016, Detective Maynard caused a subpoena to be served to T-Mobile USA, INC., requesting all available account subscriber information for IP address 2607:fb90:4092:f7e1:622d:2a87:975c:eac7. I reviewed the responsive documents received by Detective Maynard on July 4, 2016, which disclosed the following information about the subscriber for IP address 2607:fb90:4092:f7e1:622d:2a87:975c:eac7:

Subscriber Name: Michael Williams

Service Address: 8985 Normandy Blvd

Jacksonville, FL 32221-6245

Telephone #: 904-729-6485

Account Number: 845963816

Subscriber Status: A

Account Name: Michael Williams

Phone Model: LG G STYLO GRAY TMUS KIT RSU

i. Detective Maynard told me that NCMEC Tip #11561767, which I reviewed, advised the phone number associated with the Google account was 904-729-6485 and the phone number was also T-Mobile.

j. On May 27th, 2016, Detective Maynard caused a subpoena to be served to T-Mobile USA, INC., requesting all available account subscriber information for phone number 904-729- 6485. Detective Maynard told me about the responsive documents received by Detective Maynard on July 4, 2016, disclosing the following information for the above referenced phone number:

Subscriber Name: Michael Williams

Service Address: 8985 Normandy Blvd

Jacksonville, FL 32221-6245

Telephone #: 904-729-6485

Account Number: 845963816

Subscriber Status: A

Account Name: Michael Williams

Phone Model: LG G STYLO GRAY TMUS KIT RSU

k. Detective Maynard conducted surveillance of the Subject Premises on multiple occasions and observed a 2010 Black Dodge four door auto Florida License 083WRW parked in the driveway at the Subject Premises. Record checks reveal that this vehicle is registered to Michael Eugene Williams listing the

address of 8985 Normandy Blvd Lot 58, Jacksonville, FL 32221. I have visited the Subject Premises and note that 8985 Normandy Boulevard is a mobile home community comprised of multiple lots. Lot 58 is in close proximity to the Subject Premises, Lot 62. Detective Maynard also physically observed Michael Williams at the Subject Premises and observed a vehicle registered to Williams as most recently as October 14, 2016.

l. On July 5, 2016, Detective Maynard applied for and received a state search warrant in the Circuit Court of the Fourth Judicial Circuit in and for Duval County, Florida for the Subject Premises.

m. On July 7, 2016, Detective Maynard conducted the state search warrant at the residence of Michael Eugene Williams located at the Subject Premises. Officers encountered Michael Eugene Williams at the Subject Premises as well as Sandra Durby, a/k/a Nam Sun Durby. Williams advised that he lived at the Subject Premises with Durby since early 2016. Durby confirmed the same. Officers seized multiple items to include one cell phone and one computer tablet that both Williams and Durby identified as belonging to Williams.

n. On July 7, 2016, Detective Maynard submitted the seized items for a computer forensics examination where numerous files containing child exploitation material were discovered on the devices. Detective Maynard reviewed the forensics examination report where she discovered that Williams had been communicating by text messaging on the seized telephone with an individual who appeared to be producing child pornography and sending the files to Williams. The

messages and files indicated that an unidentified mother was producing files of child pornography of her own child in return for money provided by Williams. The unidentified subject phone number communicating with Williams' phone was 214-695-8630.

o. On August 29, 2016, Detective Maynard conducted an internet search on the phone number of 214-695-8630 and determined that it resolved to AT&T.

p. On August 29, 2016, Detective Maynard caused a subpoena to be served to AT&T Internet Services, requesting customer service records, subscriber, billing and credit information for telephone number 214-695-8630 from June 4, 2016 1:20:32UTC to July 6, 2016, at 8:25:05UTC. I reviewed the responsive documents received by Detective Maynard on October 4, 2016, which disclosed the following information about the subscriber for telephone number 214-695-8630:

Financially Liable Party:

Name: Philip Priest

Credit Address: 215 Weeks Rd Lot 14A, Cleburne, TX, 76031

User Information:

MSISDN: (214)695-8630

Name: Linzi S [REDACTED]¹

User Address: 493 Vincent St, Cedar Hill, TX, 75104

¹ I have redacted the last name to protect the identity of the minor victim given the aforementioned familial relationship and Linzi S.

24. On October 5, 2016, I conducted a query of the State of Florida Drivers and Vehicle Identification Database (DAVID), which indicated that an individual named Michael Eugene Williams, with a date of birth of January 28, 1957, resides at the address of 8985 Normandy Boulevard Lot 58, Jacksonville, FL 32221, and has a driver's license issued 06/09/2011.

25. On October 5, 2016, I reviewed the forensics examination report of Williams's phone and observed multiple text communications between Williams's phone number of 904-729-6485, and Linzi S [REDACTED]'s phone number of 214-695-8630. I observed approximately 337 text messages sent and received by the above listed numbers from January 19, 2016, to July 7, 2016. Numerous messages sent by Williams's phone appear to be requests for S [REDACTED] to send pornographic pictures and videos of a child named "L [REDACTED]." Additional messages pertain to S [REDACTED] sending files containing child exploitive material and requesting money to be sent in exchange for the pictures and videos sent.

26. Listed below are two of the messages I observed in the forensics report sent by Williams's phone number of 904-729-6485 to S [REDACTED]'s phone number of 214-695-8630 on March 9, 2016:

"Baby girl you know you make daddy really hard allow me to look deep inside your little girls kitty cat is so pretty and pink but I still would love you to make that video for me showing me how close you are to your daughter with your tongue and show me with your little finger inside her little kitty I don't think I could ask for anything else"

“Sure could you take one more with your lil finger going inside her kitty and you massaging her clit? And if you lick her kitty I will make it 50 dollars”

27. I reviewed the files sent by S[REDACTED]'s phone number of 214-695-8630 to Williams's phone number of 904-729-6485. Based on my training and experience, I believe the files depicts at least one minor engaged in sexually explicit conduct, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256. Described below are three of the files that Williams's phone received:

FROM: 2146958630
TO: 9047296485
TIMESTAMP: 6/23/2016 8:22:29PM (UTC-4)
TITLE: received 1131909263499119.jpeg

DESCRIPTION: The file is a still image at close range of a very young prepubescent female child's genitalia. The child is bent over exposing her vagina and anus as an adult hand is near the child's body apparently making a sign or gesture by elongating the thumb and pinky finger. The image of the very young pre-pubescent female child's vagina and anus is within view and the focal point of the image. The torso and face of the child is not showing.

FROM: 2146958630
TO: 9047296485
TIMESTAMP: 6/23/2016 9:18:11PM (UTC-4)
TITLE: IMAG0140.jpg

DESCRIPTION: The file is a still image at close range of a very young prepubescent female child's genitalia. The child appears to be lying down on her back with her legs together on top of what appears to be a multicolored quilt. Only the child's torso, genitalia, and upper thigh area are visible. The image of the very young pre-pubescent female child's vagina is within view and the focal point of the image.

FROM: 2146958630

TO: 9047296485

TIMESTAMP: 6/23/2016 9:18:11PM (UTC-4)

TITLE: IMAG0144.jpg

DESCRIPTION: The file is a still image at extremely close range of a very young prepubescent female child's genitalia. The child appears to be lying down on her back with her legs spread apart on top of what appears to be a multicolored quilt. Only the child's genitalia, lower abdomen, and buttocks area are visible. The image of the very young pre-pubescent female child's vagina is within view and the focal point of the image.

28. On October 5, 2016, I contacted HSI-Dallas regarding the investigation and live victim. Detective Maynard and I briefed HSI-Dallas Special Agent Kyle Kuykendall on the investigation and provided the investigative material.

29. On October 19, 2016, I spoke with HSI-Dallas Special Agent Kuykendall and he told me:

a. Special Agent Kuykendall identified Linzi S [REDACTED] by her married name of Linzi L [REDACTED] S [REDACTED], date of birth [REDACTED]/[REDACTED]/1988 residing at [REDACTED], Cleburne, TX, 76031.

b. On October 6, 2016, Detective Wesley Mackey, Cleburne Police Department, applied for and received a state search warrant in the 413th District Court of Texas in Johnson County for the residence of [REDACTED], Cleburne, TX, 76031.

c. On October 6, 2016, officers executed the state search warrant at the residence. Officers seized multiple items to include one cell phone belonging to S [REDACTED]. During a post-miranda interview S [REDACTED] admitted to producing child pornography of her 3-year-old daughter and sending the same to Williams in exchange for money. The officers and Texas child protective services were able to locate and rescue the child victim.

d. S [REDACTED] stated during the interview that she met Michael Williams online and continued to converse by text messaging. S [REDACTED] said he sent the explicit files to Williams in return for money. S [REDACTED] advised she sent Williams an estimated 50 files, some of which containing explicit material. S [REDACTED] claimed she received multiple payments from Williams over several months totaling approximately \$200 by way of Western Union. S [REDACTED] claimed Williams had sent some nude photos of himself to her. S [REDACTED] said, "last time I talked to him (Williams) was in September." S [REDACTED] stated she most recently communicated with Williams via Kik Messenger.

e. Bobby S [REDACTED], husband of Linzi S [REDACTED], was residing at the residence and interviewed by the officers as well.

30. On October 19, 2016, I caused a Department of Homeland Security Summons to be issued to Western Union Financial Services, Inc. requesting records pertaining to the subjects of this investigation. On the same day I received the results of the request that stated the following financial transactions were sent from Michael Williams having telephone number "9047296485" and address "8985 Normandy Blvd, Jax, FL, 32221 to Bobby S [REDACTED] having address [REDACTED] (or Lot [REDACTED]), Cleburne, TX, 76031 or 76033:

Send Date	Amount \$
-----------	-----------

9/30/2016	30.00
-----------	-------

9/8/2016	40.00
----------	-------

8/29/2016	40.00
-----------	-------

6/24/2016	45.00
-----------	-------

3/24/2016	45.00
-----------	-------

3/9/2016	40.00
----------	-------

2/25/2016	20.00
-----------	-------

2/16/2016	45.00
-----------	-------

10/22/2015	40.00
------------	-------

10/6/2015	40.00
-----------	-------

9/28/2015	40.00
-----------	-------

9/14/2015	40.00
-----------	-------

9/1/2015 45.00
8/24/2015 25.00
8/17/2015 30.00
8/15/2015 45.00
7/31/2015 45.00
7/17/2015 40.00
6/30/2015 50.00

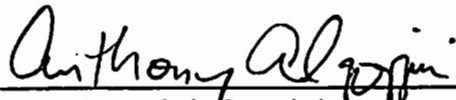
31. I observed that three of the financial transactions conducted took place well after the date that Detective Maynard and detectives with the Jacksonville Sheriff's Office conducted the state search warrant at Williams's residence. As a result, I have probable cause to believe that Williams has continued to send money to Linzi S [REDACTED] for the receipt of visual depictions of a minor engaging in sexually explicit conduct, even after Williams was contacted by law enforcement.

CONCLUSION

32. Based on the foregoing, I have probable cause to believe that one or more individuals has used and/or is using one or more computers and/or electronic storage media located at the Subject Premises at 8985 Normandy Boulevard Lot 62, Jacksonville, FL 32221, 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.

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



Anthony Algozzini, Special Agent
Homeland Security Investigations- Jacksonville

Subscribed and sworn to before me this 20th day of October, 2016, at Jacksonville, Florida.



MONTE C. RICHARDSON
United States Magistrate Judge

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is a residence located at 8985 Normandy Boulevard Lot 62, Jacksonville, FL 32221, identified as a single story double wide mobile home that is gray in color. The first floor primarily consists of gray painted siding. There is a concrete driveway to the residence which is positioned at an angle on the lot. There are six steps facing south that lead up to a gate before accessing a covered front porch to access the front door facing west. The numbers "62" are visible on the south and west corners of the residence. The residences on either side near the premises are single wide mobile homes. The back door is on the east side of the residence at the north side of the trailer with a small wood porch. The back yard has a wood privacy fence to the north separating the mobile home park from the adjoining neighborhood but no fences are present between each mobile home. There are no other residences in the immediate area that look the same.

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, personal digital assistants (PDA), digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images), computer-related documentation, computer passwords and data-security devices, videotapes, video recording devices, video recording players, and video display monitors that are or may be used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography or child erotica.

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

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs

and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

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

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

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

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and

electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

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

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

12. Any and all cameras, film, videotapes or other photographic equipment that may be or are used to: visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the

United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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