AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Anthony Davis Stagnitta

Case No. 3:18-mj- 1157-PDB

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of December 3, 2017 in the county of Duval in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Knowing distribution of child pornography over the internet

This criminal complaint is based on these facts:

See attached.

☑ Continued on the attached sheet.

Complainant's signature

ASHLEY WILSON, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/30/2018

Judge's signature

City and state: Jacksonville, Florida

PATRICIA D. BARKSDALE, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Ashley Wilson, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), an agency of the United States Department of Homeland Security (DHS), and have been so employed since October 2007. I am currently assigned to the Office of the Assistant Special Agent in Charge Jacksonville, Florida, where I conduct a variety of investigations. Prior to this assignment, I was assigned to the Office of the Deputy Special Agent in Charge Laredo, Texas for approximately six years also as a Special Agent. I have a Bachelor's degree in Criminal Justice. I am a law enforcement officer of the United States and am thus authorized by law to engage in or supervise the prevention, detection, investigation or prosecution of violations of federal criminal law. I am responsible for enforcing federal criminal statutes under the jurisdiction of HSI, including violations of law involving the exploitation of children. I participated in a 22-week training program at the Federal Law Enforcement Training Center in Brunswick, Georgia, which included the Criminal Investigator Training Program and ICE Special Agent Training. In my capacity as a Special Agent, I have participated in numerous types of investigations, during which I conducted or participated in physical surveillance, undercover transactions and operations, historical investigations, and other complex investigations. Since becoming a

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

2. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the possession, collection, production, receipt, distribution, and transportation of images and videos depicting the sexual exploitation of children, and the solicitation and extortion of children to produce sexually explicit depictions of themselves. I have been involved in searches of residences pertaining to the possession, collection, production, and/or transportation of child exploitation materials through either the execution of search warrants or through the subject providing written consent to permit a search to be conducted.

3. The statements contained in this affidavit are based on my personal knowledge, as well as on information provided to me by experienced Special Agents and other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of establishing probable cause for the filing of a criminal complaint, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that ANTHONY DAVIS STAGNITTA has committed a violation of 18 U.S.C. § 2252(a)(2), that is, knowing distribution of child pornography over the internet.

4. I make this affidavit in support of a criminal complaint against ANTHONY DAVIS STAGNITTA, that is, on or about December 3, 2017, in the Middle District of Florida and elsewhere, ANTHONY DAVIS STAGNITTA, did knowingly distribute visual depictions using any means and facility of interstate and foreign commerce by any means, that is, by computer via the internet, when the production of the visual depictions each involved the use of a minor engaging in sexually explicit conduct, and the visual depictions were of such conduct, the visual depictions being specifically identified in the computer files titled "d7845dc0-6aa0-45e6-b44c-e6c27738d2f3," in violation of 18 U.S.C. § 2252(a)(2).

5. On April 27, 2018, I applied for and obtained a federal search warrant for the residence located at 10721 Indies Drive North, Jacksonville, Florida 32246, believed to be occupied by ANTHONY DAVIS STAGNITTA. I was the affiant for the affidavit in support of the application for this search warrant, and I am familiar with the facts contained therein. A certified copy of the application and affidavit for this search warrant is attached as Exhibit A, and the facts and information contained therein is hereby incorporated by reference herein. This warrant authorized the search of this residence for fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, that is, receipt, distribution, and possession of child pornography. This search warrant was issued

by United States Magistrate Judge Patricia D. Barksdale in Case No. 3:18-mj-1153-PDB.

6. On April 30, 2018, at approximately 6:05 a.m., I, together with other HSI agents and law enforcement personnel, executed this search warrant at the residence located at 10721 Indies Drive North, Jacksonville, Florida 32246.

7. Anthony Davis STAGNITTA was located inside the residence, and temporarily detained while the residence was cleared. During that time, STAGNITTA asked me if he could ask some questions about what was going on. I told him once the residence was cleared, we would be able to talk. Once the residence was cleared, STAGNITTA was released and HSI Special Agent Anthony Algozzini approached him for a possible interview. STAGNITTA agreed to join us in our HSI vehicle.

8. HSI Special Agent Algozzini and STAGNITTA walked to the HSI vehicle I was sitting in and STAGNITTA sat in the front passenger seat. I introduced myself as a Special Agent and presented my badge and credentials to STAGNITTA. I told STAGNITTA I wanted to ask him some questions and advised him of his rights. STAGNITTA was given a Statement of Rights form to review and he waived his rights by signing the bottom portion of the form. STAGNITTA agreed to talk to us without an attorney present and provided, among other things, the following information:

(a) STAGNITTA has rented the current residence for approximately two years with his brother and two other roommates. STAGNITTA's room is the big room in the hallway and he confirmed which bedroom was his when I showed him pictures I took earlier that morning. STAGNITTA has two devices, one Samsung Galaxy S7 cell phone and one Dell laptop. Both of the devices were found lying on the floor next to the bed in his bedroom, and STAGNITTA acknowledged ownership of both devices.

(b) STAGNITTA uses AT&T for internet services and the account is in his name. The residence has Wi-Fi and it is password protected. The secured network is called "ATT3dbh9Tz".

(c) STAGNITTA uses the Internet for various activities to include listening to music, and playing video games. STAGNITTA has a Facebook and Snapchat account.

(d) When asked if he had a Kik account, STAGNITTA stated he used it several years ago but could not remember an associated username or email address. When asked if the username "whatsa9" sounded familiar to him, STAGNITTA hesitated and acknowledged that he did. When asked if the email address "spartan23549@gmail.com" sounded familiar to him, STAGNITTA said it was one of his old email addresses and he currently uses it for gaming purposes.

(e) I told STAGNITTA I knew he was recently using the Kik

application with the username "whatsa9" and email address spartan23549@gmail.com. STAGNITTA acknowledged and admitted to using Kik with username "whatsa9" and email address spartan2354@gmail.com. STAGNITTA used Kik to view pornographic material and was a member of group chats that discussed child pornography. STAGNITTA admitted to being a member of approximately 10 group chats that traded child pornography. STAGNITTA used the Kik application to send and receive videos containing child pornography. STAGNITTA sent the videos containing child pornography to other Kik users via private messaging or posted the videos in the group chats. STAGNITTA initially admitted to receiving approximately 15 images and videos of child pornography and later stated he has received approximately 150 files containing child pornography. STAGNITTA used the Kik application on his cell phone to send and receive child pornography.

(f) I showed STAGNITTA both of the video files he sent to the Kik group chat and that is referenced in attached Exhibit A. The first video file, titled "03ad937a-c90a-4759-b073-8872910e7e3c" was sent on December 1, 2017. STAGNITTA said he has seen the video and remembers it. STAGNITTA said, "It might have been posted to one of the groups or it might have been sent to me, I'm not 100% sure." I told STAGNITTA he sent the video file to the group chat on December 1, 2017 from his cell phone. HSI SA Algozzini asked STAGNITTA if

that was accurate and STAGNITTA said "yes." When asked if he masturbated to the video, STAGNITTA said "At the time, probably yes". The second video file, titled "d7845dc0-6aa0-45e6-b44c-e6c27738d2f3", was sent on December 3, 2017 and that is referenced in attached Exhibit A. STAGNITTA said he has seen the video and remembers it. STAGNITTA said, "Yeah. If I received it, then I probably sent it. I don't know if it was posted in a group or if it was sent to me personally."

9. A forensic preview examination of STAGNITTA's cell phone, a Samsung Galaxy, was conducted by HSI Computer Forensic Analyst (CFA) Van Wilson, who advised me of the results. I learned that at least 25 images depicting child pornography were discovered on this device. I viewed one of these images, titled "QOhjjQgR.jpg" and observed that it is a color picture depicting a prepubescent female child and an adult male. The female child is completely nude and shown from head to mid-thigh level, while only the penis is shown of the adult male. The picture depicts the female child laying on her back on what appears to be a bed with pillow and red blanket. The picture depicts the adult male's erect penis penetrating the female child's genitals. I viewed another one of these images, titled "wXQWwS6S.jpg" and observed that it is a color picture depicting an adult male and a prepubescent female child. Both the adult male and female child are nude from the waist down. The picture depicts the adult male laying back on a blue colored sofa with the female child sitting on top of the male's abdomen region. The

picture depicts the adult male's erect penis attempting to penetrate the female child's genitals. Based on my training and experience, I believe that each of these images depict at least one minor engaging in sexually explicit conduct, that is, genital-genital intercourse.

10. After the conclusion of the interview of STAGNITTA, I contacted Assistant United States Attorney D. Rodney Brown, who authorized me to arrest STAGNITTA for knowing distribution of child pornography. Shortly thereafter, I placed STAGNITTA under arrest.

11. Based upon the foregoing facts, I have probable cause to believe that on or about December 3, 2017, in the Middle District of Florida and elsewhere, defendant, ANTHONY DAVIS STAGNITTA, did knowingly distribute a visual depiction using any means and facility of interstate and foreign commerce by any means, that is, by computer via the internet, when the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct, and the visual depictions were of such conduct, the visual depictions being specifically

identified in the computer file titled "d7845dc0-6aa0-45e6-b44c-e6c27738d2f3," in violation of 18 U.S.C. § 2252(a)(2).

ASHLEY WILSON, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me this
30th day of April, 2018, at Jacksonville, Florida.

PATRICIA D. BARKSDALE
United States Magistrate Judge

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

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

A residence located at 10721 Indies Drive North, Jacksonville, Florida 32246, more particularly described in Attachment A

Case No. 3:18-mj- 1153-PDB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
A residence located at 10721 Indies Drive North, Jacksonville, Florida 32246, more particularly described in Attachment A,

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

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252 & 2252A	Receipt, distribution, and possession of child pornography.

The application is based on these facts:

See attached Affidavit.

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

Applicant's signature

HSI Special Agent Ashley Wilson
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/27/2018 2:35 pm

Judge's signature

City and state: Jacksonville, Florida

Patricia D. Barksdale, United States Magistrate Judge
Printed name and title

Exhibit A

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is a residence located at 10721 Indies Drive North, Jacksonville, Florida 32246, and is situated on the north side of Indies Drive North. The residence is a one-story tan house with a side door on the east side of the house underneath a porch. There is a sidewalk in front of the residence that leads to a second side door on the west side of the residence. There are no doors and three large windows on the front side of the house. Brown colored shingles cover the roof and a paved, single lane driveway extends from the street to southeast side of the residence. The numerals "10721" are displayed in white on a black mailbox that is attached to two white posts. The mailbox is placed on the front edge of the front yard next to the paved driveway. The property is surrounded by a chain link fence.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

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

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

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

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

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 advertising for, soliciting, distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

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

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

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

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

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

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

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

electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises to be searched, including rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

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

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

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Ashley Wilson, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), an agency of the United States Department of Homeland Security (DHS), and have been so employed since October 2007. I am currently assigned to the Office of the Assistant Special Agent in Charge Jacksonville, Florida, where I conduct a variety of investigations. Prior to this assignment, I was assigned to the Office of the Deputy Special Agent in Charge Laredo, Texas for approximately six years also as a Special Agent. I have a Bachelor's degree in Criminal Justice. I am a law enforcement officer of the United States and am thus authorized by law to engage in or supervise the prevention, detection, investigation or prosecution of violations of federal criminal law. I am responsible for enforcing federal criminal statutes under the jurisdiction of HSI, including violations of law involving the exploitation of children. I participated in a 22-week training program at the Federal Law Enforcement Training Center in Brunswick, Georgia, which included the Criminal Investigator Training Program and ICE Special Agent Training. In my capacity as a Special Agent, I have participated in numerous types of investigations, during which I conducted or participated in physical surveillance, undercover transactions and operations, historical investigations, and other complex investigations. Since becoming a Special

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

2. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the possession, collection, production, receipt, distribution, and transportation of images and videos depicting the sexual exploitation of children, and the solicitation and extortion of children to produce sexually explicit depictions of themselves. I have been involved in searches of residences pertaining to the possession, collection, production, and/or transportation of child exploitation materials through either the execution of search warrants or through the subject providing written consent to permit a search to be conducted.

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/or 2252A, is present in the 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, computer forensic examiners, and at least one federal prosecutor, I know the following:

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

b. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

c. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any

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

d. 18 U.S.C. § 2252A(a)(l) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(3) prohibits a person from knowingly reproducing child pornography for distribution through the mails or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing

with intent to view any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

e. The internet is a facility of interstate commerce.

DEFINITIONS

5. The following definitions apply to this Affidavit:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

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

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

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

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

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

video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

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

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

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

m. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable

storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

COMPUTERS AND CHILD PORNOGRAPHY

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

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

8. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, images and videos can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

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

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

11. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, and Google, among others. The online services allow 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 experienced law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were

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

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

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

a. Computer storage devices *(e.g.*, hard drives, compact disks ("CDs"), 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[1], 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

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

and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

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

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

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest in children and associated behavior. The different Internet based vehicles used by such individuals to communicate with each

other include, but are not limited to, P2P, email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

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

f. Many individuals who collect child pornography rarely, if dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other like-minded individuals over the Internet. As such, they tend to maintain

or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. These individuals may protect their illicit materials by passwords, encryption, and other security measures; save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted; or send it to third party image storage sites via the Internet. Based on my training and experience, as well as my conversations with other experienced law enforcement officers who conduct child exploitation investigations, I know that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often maintain and/or possess the items listed in Attachment B.

15. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials. For example, I am aware of an investigation by the FBI in Jacksonville 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 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. Based on my training and experience, I also know that, with the development of faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. However, as referenced above, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favorite images involving a particular child or act is often maintained on the device.

17. Based on my training and experience, I know that within the last several years, individuals who have a sexual interest in minor children have used the internet and internet-enabled devices with increasing frequency to make contact with and attempt to establish relationships with potential child victims. These individuals

may perceive that the internet provides some degree of anonymity and safety from prosecution. Because more and more children are using the internet and internet enabled devices, these individuals potentially expose more and more child victims to online sexual exploitation. These individuals may contact potential child victims through social networking websites such as Facebook and Twitter, or may engage in online conversations with children through text messaging and email. During these online conversations, photographic images and links to internet websites can be easily exchanged between the individual and the targeted child. Based on my training and experience, I know that when such an individual uses text messaging, email, or other websites to have online contact with children, the internet-enabled device used, whether it is a computer, a cellular telephone, a "smart" phone such as an "iPhone," or a tablet such as an "iPad," often saves and maintains evidence of such contacts. This evidence can often be extracted and examined by a trained forensic examiner.

KIK MESSENGER APPLICATION INFORMATION

18. The following information has been provided to me by other experienced law enforcement officers and also comes from online research that I have conducted as well as my training and experience. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app from the Canadian company Kik Interactive, available free of charge on iOS and Android operating systems. It is a social networking application which permits a user to trade and disseminate various forms of digital media, while utilizing a cellphone. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009

and according to their website, which I have viewed, was designed to "shift the center of computing from the PC to the phone." Kik is a free service easily downloaded as an application from the Internet. Kik Messenger is a feature within Kik that allows its users to communicate to selected friends as well as browse and share any web site content with those whom the user selects, while still on the Kik platform. Unlike other messenging apps, Kik usernames - not phone numbers - are the basis for Kik user accounts. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to "Groups." Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture themed ideas as well as illicit/illegal themed ideas. Following the creation of Kik, other software developers have created similar programs, such as "Pikek" which is a modified version of the Kik application. Pikek actually interfaces with Kik, however, enables the user more features that the original Kik does not offer, such as the ability to seek out and find "Groups." Based on my training and experience, I know that Kik is often used for illegal purposes, including the distribution of child pornography, because of the high degree of anonymity that is afforded to the user during the use of the Kik application.

BACKGROUND OF INVESTIGATION AND FACTS ESTABLISHING PROBABLE CAUSE

19. I make this affidavit in support of a search warrant for the residence located at 10721 Indies Drive North, Jacksonville, Florida 32246 that I believe to be currently occupied by Anthony Davis STAGNITTA (date of birth [redacted]). This affidavit is based on information provided to me both verbally and in written documentation from other law enforcement officers and personnel, including HSI Special Agent Ryan Eggland assigned to the HSI Orlando office, as well as through investigation that I personally conducted as set forth herein. I have physically seen and taken photographs of the residence. I have personally observed the residence, and it appears as set forth in Attachment A.

20. In February 2018, I learned that federal agents with the HSI Office in Ottawa, Canada receive monthly reports from Kik that include profile information for all Kik application users that are believed to be sharing, uploading or discussing child pornography based on shared images, profile information, text conversations.

21. On February 9, 2018, SA Eggland contacted me by email and stated in substance he received several investigative leads and referrals involving Kik from the HSI Office in Canada. SA Eggland explained in the email, and in several telephone conversations, that some of the leads were sent to the HSI Orlando office because the cell phone IP addresses resolved back to the cell phone companies' hubs. One of the leads that he (SA Eggland) received involved Kik username "whatsa9" who used the

Kik application to distribute two videos depicting the sexual exploitation of children, also known and referred to as child pornography. According to information received from Kik as contained in SA Eggland's email and referenced in our telephone conversations, the first name on this particular account is "Jake" and the last name is "Sanders." The email address associated to this Kik account is spartan23549@gmail.com. According to SA Eggland, Kik also captured the name "Tony Stagnitta" with a date of birth of [redacted] under the Kik account information.

22. According to SA Eggland, he conducted an initial investigation which included reviewing the information sent by Kik, conducting open source research on Facebook and searching other investigative databases. SA Eggland also reviewed the two videos that he received from Kik that depicted child pornography. SA Eggland discovered a Facebook page in the name of "Tony Stagnitta" with a profile picture of male with dark hair playing a trumpet. Several posts on the Facebook page of "Tony Stagnitta" depict the same adult male as identified in the Driver and Vehicle Information Database, with the date of birth (DOB) [redacted]. Additionally, listed under the "About" section on the Facebook page on Tony Stagnitta, SA Eggland discovered was the phrase "Studies at University of Florida from 2015 to present." After this initial investigation, SA Eggland determined the Kik username "whatsa9" appeared to be associated with Anthony Davis STAGNITTA, who has an associated address in St. Petersburg, Florida and is attending the University of North Florida located in Jacksonville. SA Eggland concluded that Kik sent the

information to the HSI Office in Canada and they forwarded the lead to him believing STAGNITTA was located somewhere in the Orlando area. Subsequently, SA Eggland forwarded this investigative lead and all associated information, including that set forth above, to me.

23. On or about February 26, 2018, I received the investigative lead and reviewed all of the information provided by Kik through SA Eggland, including the two videos containing child pornography distributed over the internet by Kik username "whatsa9." Based on my training and experience, as well as conversations with other experienced Special Agents, I believe that both videos depicted minors engaged in sexually explicit conduct. I also obtained the unique SHA-1 value for each of the video files. Based on my training and experience, I know that a SHA-1 value is a unique identifier based on an algorithm that is specific to a particular video and/or image, and further that SHA-1 value are used by law enforcement to identify images and videos that depict child pornography. On or about March 5, 2018, I, along with HSI SA Nathan Smith, reviewed the case documents received from SA Eggland in more detail. Kik provided information to HSI, that I had reviewed, about the device type used by "whatsa9," which was a Samsung Android, as well as a series of IP addresses from November 7, 2017 through December 8, 2017 that resolved to Kik user "whatsa9."

24. According to Kik records and logs that I have reviewed, user "whatsa9" was in a public group chat with five (5) other users and the group code for the chat was "#nepibaby". On November 24, 2017 at 14:39:18 UTC (Coordinated Universal

Time), user "markforyoung," one of the five members in the group chat, sent the following text message to the group: "Hi I'm Mark, greedy to see db stuff please, also UK sex offender contacts, meets... Need baby boy interests... Painful use. Squealing." On November 24, 2017 at 14:47:16 UTC, user "markforyoung" sent the following text message to the group: "Anymore like minded groups". On November 24, 2017 at 16:18:38 UTC, user "markforyoung" texted the following message to the group: "Shame many paedo guys drug the toddlers...as nice to hear them screaming and squeling". On November 26, 2017 at 16:21:55 UTC, user "whatsa9" sent the following text message to the other members of the group: "Anyone down to trade?". On November 30, 2017 at 00:26:00 UTC, user "whatsa9" sent the following text message to the group: "Anyone trade?". As part of my review of IP addresses provided by Kik that resolved to user "whatsa9", I learned that IP address 108.225.175.79 resolved to user "whatsa9" between the times of November 29, 2017 at 23:05:39 and November 30, 2017 at 01:20:15, during which time period the user "whatsa9" sent the above message.

25. Further review of the Kik logs and records revealed that on December 1, 2017 at 14:56:06 UTC, user "whatsa9" sent a video to the group using the internet. On December 3, 2017 at 05:53:09 UTC, user "whatsa9" sent a second video to the group using the internet.

26. I conducted a query of Maxmind, a publicly available online resource, and it was determined AT&T U-verse was the owner of IP address 108.225.175.79.

27. On March 28, 2018, I requested and caused an administrative summons to be issued to AT&T requesting subscriber information for IP address 108.225.175.79 between November 7, 2017 at 13:59:35 UTC and November 30, 2017 at 01:20:15 UTC. On April 17, 2018, AT&T provided the requested information to me and I reviewed it. The information provided listed the account as open with an associated phone number of 727-773-7880, and the subscriber as Anthony Stagnitta residing at 10721 N Indies Drive, Jacksonville, FL 32246.

28. On April 4, 2018, I conducted additional research and discovered STAGNITTA has an active account with Jacksonville Electric Authority (JEA). The name listed on the account is Anthony D Stagnitta and the service address is 10721 Indies Drive N, Jacksonville, FL 32246.

29. On April 26, 2018, I viewed the video files that were provided by Kik and sent over the internet by Kik user "whatsa9". The two videos distributed by Kik user "whatsa9" over the internet using the Kik application on the dates listed below are described as follows:

TITLE: 03ad937a-c90a-4759-b073-8872910e7e3c

SHA-1: 5WHF54HW7Y3SUSTPJFKCDGH3W7OVNGCT

DATE: December 1, 2017

DESCRIPTION: This is a 53 second color video with no sound which depicts an erect penis ejaculating on the face on an infant wearing a pink bib. After ejaculating on the infant, the person operating the camera zooms in on the infant's face. Based on my training and experience, I believe that this video depicts at least

one minor engaged in sexually explicit conduct, that is, the lascivious exhibition of a a person's genitalia, sexual intercourse, and masturbation, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256. .

TITLE: d7845dc0-6aa0-45e6-b44c-e6c27738d2f3

SHA-1: EZ7ATCENCCQJYMAKLAZFNSRXVFTJES32

DATE: December 3, 2017

DESCRIPTION: This is a one (1) minute and 21 second color video with no sound which depicts a naked infant propped up on a pillow on a couch. An male individual with an erect penis stands over the infant and begins to masturbate. The male spreads the infant's legs and touches the infant's penis with his erect penis. The male then forces his erect penis into the infant's mouth and continues to masturbate until he ejaculates into the infant's mouth. During this time, the infant's face and upper body become red and purple. The male removes his penis from the infant's mouth and rubs the end of his penis over the lips of the infant. Based on my training and experience, I believe that this video depicts at least one minor engaged in sexually explicit conduct, that is, genital-genital sexual intercourse, oral-genital sexual intercourse, and the lascivious exhibition of a minor child's genitalia, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

30. On April 26, 2018, I conducted visual surveillance at the residence located at 10721 Indies Drive North, Jacksonville, Florida 32246. At approximately 7:00 p.m., I observed a gold Mazda 3 vehicle, bearing Florida license plate EEX-

A52, drive past my location on Indies Drive North and pull into the driveway at the residence located at 10721 Indies Drive North. As the vehicle traveled past me, I recognized that the male driver was STAGNITTA. I am familiar with his appearance as I have reviewed numerous photos of STAGNITTA on his Facebook page and have also seen his driver license photo in the Florida Driver and Vehicle Information Database. I also caused an updated query to be run on the JEA database on April 27, 2018, and I have reviewed the results. This query showed that the name listed on the account at the 10721 Indies Drive North residence is Anthony D Stagnitta and the service address is still 10721 Indies Drive N, Jacksonville, FL 32246.

CONCLUSION

31. Based on the foregoing, I have probable cause to believe that one or more individuals has used and is using one or more computer devices, smart phones, and/or electronic storage media located in the residence located at 10721 Indies Drive North, Jacksonville, Florida 32246, more fully described in Attachment A to this affidavit to, among other things, distribute, 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/or 2252A. Additionally, I have probable cause to believe that fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including at least one computer device and/or other electronic storage media containing images and/or video depicting child pornography, and the items more fully described in

Attachment B to this affidavit (which is incorporated by reference herein), will be located in this residence.

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

ASHLEY WILSON, Special Agent
Homeland Security Investigations

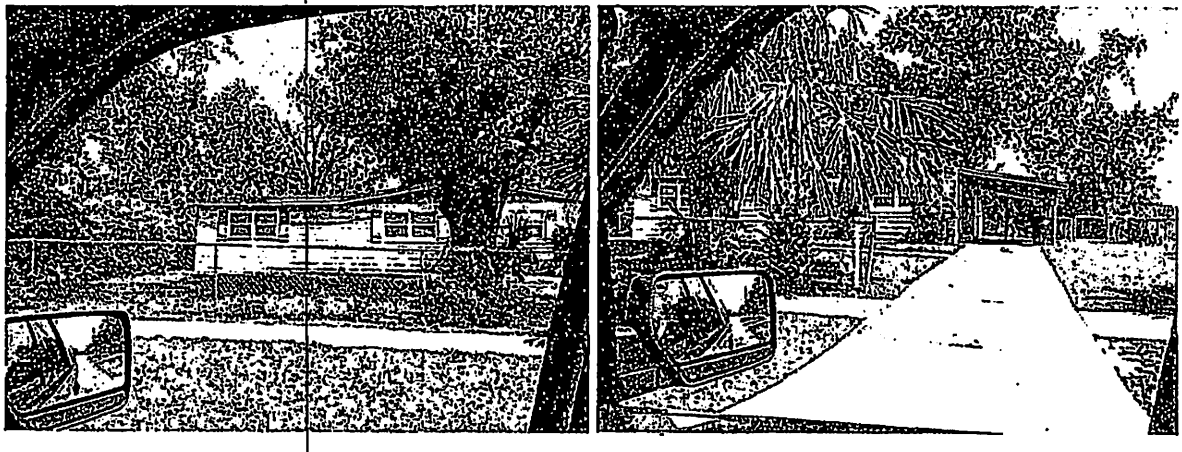
Subscribed and sworn to before me this
27th day of April, 2018, at Jacksonville, Florida.

PATRICIA D. BARKSDALE
United States Magistrate Judge

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is a residence located at 10721 Indies Drive North, Jacksonville, Florida 32246, and is situated on the north side of Indies Drive North. The residence is a one-story tan house with a side door on the east side of the house underneath a porch. There is a sidewalk in front of the residence that leads to a second side door on the west side of the residence. There are no doors and three large windows on the front side of the house. Brown colored shingles cover the roof and a paved, single lane driveway extends from the street to southeast side of the residence. The numerals "10721" are displayed in white on a black mailbox that is attached to two white posts. The mailbox is placed on the front edge of the front yard next to the paved driveway. The property is surrounded by a chain link fence.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

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

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

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

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

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 advertising for, soliciting, distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

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

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

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

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

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

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

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

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

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

electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises to be searched, including rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

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

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