

AO (Rev. 5/85) Criminal Complaint

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
JACKSONVILLE DIVISION

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

vs.

Case Number: 3:17-mj- 1138-JBT

JASON JAMES NEIHEISEL

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about February 7, 2016, at Jacksonville, in the Middle District of Florida, defendant, JASON JAMES NEIHEISEL 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 depiction was of such conduct, the visual depiction being specifically identified in the computer file titled "bathtime with daddy-3yo girl ped.mpg," in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(b)(1).

I further state that I am a Special Agent with Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

  
\_\_\_\_\_  
Signature of Complainant  
NICHOLAS PRIVETTE, Special Agent  
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

May 3<sup>rd</sup>, 2017

at

Jacksonville, Florida

JOEL B. TOOMEY  
United States Magistrate Judge  
\_\_\_\_\_  
Name & Title of Judicial Officer

  
\_\_\_\_\_  
Signature of Judicial Officer

**AFFIDAVIT**

I, Nicholas Privette, being duly sworn, state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since August 2016 when I began my law enforcement training at the FBI Academy in Quantico, Virginia. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes and child exploitation. Prior to this assignment, I was employed with the United States Army for approximately 12 years as an Infantry Officer and most recently held the position of Company Commander. I have a Bachelor of Science degree in Information Engineering and a Master of Science degree in Organizational Leadership. Since becoming a Special Agent, I have worked with experienced Special Agents, as well as other law enforcement officers and personnel, including an experienced Assistant United States Attorney, all of whom have considerable experience investigating and prosecuting child exploitation offenses. A substantial portion of my duties are dedicated to investigating and assisting with cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. In the performance of my duties, I have assisted in the investigation of matters involving the possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography. I have been involved in searches of residences, computers, and digital media pertaining to the advertisement for, possession, collection, production,

and/or transportation of child pornography, through either the execution of search warrants or through the subject providing written consent to permit a search.

2. I have 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 which criminalize the possession, receipt, and transmission of child pornography, that is, visual images depicting minors engaged in sexually explicit conduct. In connection with such investigations, I have participated in interviews of subjects, witnesses, and potential victims, and I have observed experienced Special Agents do the same and serve in the role of case agents. I am a member of the FBI Jacksonville Field Office's Child Exploitation Task Force, which comprised of federal, state, and local law enforcement agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on my personal knowledge, as well as on information provided to me by experienced Special Agents and other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of establishing probable cause for the filing of a criminal

complaint, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that JASON JAMES NEIHEISEL has committed a violation of Title 18, United States Code, Section 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 JASON JAMES NEIHEISEL, that is, on or about February 7, 2016, at Jacksonville, in the Middle District of Florida, JASON JAMES NEIHEISEL, 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 depiction was of such conduct, the visual depiction being specifically identified in the computer file titled "bathtime with daddy-3yo girl ped.mpg", in violation of Title 18, United States Code, Section 2252(a)(2).

5. On April 13, 2017, I applied for and obtained a federal search warrant for a silver-colored Microsoft Surface computer tablet, with no visible serial number, that was obtained from JASON JAMES NEIHEISEL at his apartment residence in Jacksonville, Florida on April 11, 2017 by me and FBI SA Jonathan MacDonald. 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<sup>1</sup>. This warrant authorized the search of the silver-colored Microsoft Surface computer tablet 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. 3:17-mj-1101-PDB.

6. A detailed narrative of the consensual interview with NEIHEISEL on April 11, 2017 is included within Exhibit A at paragraphs 31 and 32. Later in the morning on April 11, 2017, NEIHEISEL called me on the FBI Jacksonville Field Office main telephone number for follow up discussion. NEIHEISEL called to “check in” and to “see what the next step is” regarding an investigation of child pornography involving him. He reiterated in substance that he desired to assist me and SA MacDonald with the investigation. When I asked if he had additional information regarding the general time frame and internet sources that he used to find and download child pornography, NEIHEISEL did not offer more specifics other than what was previously discussed during the in-person interview. NEIHEISEL stated that believed that other child pornography content could be

---

<sup>1</sup> Certain identifying information has been redacted from the affidavit in support of the application for the search warrant to protect the privacy of persons referred to therein.

found on similar websites and file sharing programs as “when I’ve found it before.” NEIHEISEL did not have any further questions at that time and indicated that he wished to schedule a follow up meeting with me, but was unsure of his schedule availability. NEIHEISEL advised me that he would review his schedule and call me back with a suggested date and time for an in-person meeting later in the week.

7. On April 12, 2017, NEIHEISEL called me on the FBI Jacksonville Field Office main telephone number to “check in.” NEIHEISEL reiterated his desire to assist with the investigation, but he did not have any further questions for me and did not have any additional information to offer. When I asked if NEIHEISEL still wished to schedule a follow up meeting with me, he said that he would like to do so. NEIHEISEL was initially unsure of his schedule availability but advised that during lunch on Friday of the same week would probably work. When asked what type of meeting (public or private) NEIHEISEL would prefer, he was unsure and did not offer a specific location. NEIHEISEL agreed to a tentative meeting time of 11:00 a.m. on Friday, April 14, 2017, pending further contact to decide on a specific meeting location.

8. On April 13, 2017, I submitted NEIHEISEL’s Microsoft Surface computer tablet referred to above to the computer forensic examiners at the FBI Jacksonville Field Office for forensic examination. Based on my conversations with Andrew Spurlock, whom I know to be an experienced FBI certified computer



forensic examiner, I learned that the Microsoft Windows operating system appeared to have been re-installed on NEIHEISEL's tablet on or about December of 2016. Upon my review of the contents of NEIHEISEL's tablet using a forensic software tool, I also discovered the following:

a. The tablet contained many artifacts, such as programs, images, and multimedia, that indicated that NEIHEISEL has used the tablet for personal use. In particular, a user profile named "Jason" was present on the tablet, with various folders and subfolders containing personal content.

b. The BitTorrent <sup>client</sup> ~~program~~ "Vuze" was installed on NEIHEISEL's tablet. It appears that the program was used to download the movie "Elf," and this fact corroborates NEIHEISEL's statement during our consensual interview on April 11, 2017.

c. There did not appear to be any child pornography content currently saved or stored on NEIHEISEL's tablet. This also corroborates NEIHEISEL's statements during our consensual interview on April 11, 2017.

9. On April 18, 2017, NEIHEISEL called me on the FBI Jacksonville Field Office main telephone number to "check in." NEIHEISEL reiterated his desire to assist with the investigation, but he did not have any further questions for me and did not have any additional information to offer. NEIHEISEL indicated in substance that he was very busy and "slammed" with work that week and agreed to

set up an in-person meeting with me the following week. NEIHEISEL agreed to a tentative meeting time of 11:30 a.m. on Tuesday, April 25, 2017, at a location in the vicinity of the St. Johns Town Center in Jacksonville, Florida. On the morning of April 25, 2017, I called NEIHEISEL on his cellular phone, and we agreed to meet at the Panera Bread restaurant in the St. Johns Town Center in Jacksonville, Florida at 11:15 a.m. that same day.

10. On April 25, 2017, SA MacDonald and I conducted a consensual interview of NEIHEISEL at Panera Bread restaurant in the St. Johns Town Center, 4720 Town Crossing Drive, Jacksonville, Florida 32246. At approximately 11:15 a.m., NEIHEISEL arrived and met us at an outdoor table at Panera Bread.

NEIHEISEL provided the following information, among other things:

a. In thinking back to the previous interview on April 11, 2017, NEIHEISEL said he “never used BitTorrent in any capacity.” However, upon refreshing his recollection of the prior interview, NEIHEISEL affirmed in substance that he had in fact used BitTorrent to download and make child pornography videos available for distribution to other users of the BitTorrent network.

b. Chat Tango is a program or application NEIHEISEL used to find child pornography and likened it to “reddit.com” of which he said, “I’m on it all the time.” In Chat Tango, users of the platform are able to send links which direct other users to cloud-based storage or servers elsewhere which house the contents of



child pornography. Likewise, other users of Chat Tango are able to click on those links and are taken to a particular location where child pornography images and videos are available to view and download. NEIHEISEL recalled his downloading of child pornography activity as, “it’s kind of dumb” and added, “you download stuff you download,” and intimated that child pornography is just out there, often with an innocuous name or title for the zip files which contain the child pornography content.

c. Unlike the Chat Tango platform in which users are able to send links to another Chat Tango user, NEIHEISEL confirmed that BitTorrent works differently. BitTorrent has a default folder created upon installation of the BitTorrent software called “downloads.” It is from this “downloads” folder that other users of BitTorrent are able to collect content which is saved in that “downloads” folder. NEIHEISEL confirmed that the child pornography videos shown to him during the prior consensual interview on April 11, 2017 were obtained by law enforcement from his “downloads” folder, and that law enforcement was able to receive those child pornography videos from his “downloads” folder not because NEIHEISEL directed law enforcement to take them, but instead because NEIHEISEL knew that he had made the child pornography videos available for distribution to anyone else on the BitTorrent network who wished to participate. He further understood and agreed that “anyone on the BitTorrent network can get

videos from the shared folder, but [NEIHEISEL] doesn't solicit others for it."

d. NEIHEISEL kept his child pornography videos in his downloads folder for more than one day but less than one month, and estimated it was likely he "kept for a week" then deleted the child pornography. NEIHEISEL deleted the child pornography videos after he "no longer needed them" and because his device could potentially be shared by other users.

e. NEIHEISEL was unaware of specific locations of children being victimized in the Jacksonville area. Other than BitTorrent, he had no knowledge of enterprise operations to coordinate the abuse of children and was also unaware of other applications, platforms, or programs other than BitTorrent and Chat Tango which are used to traffic child pornography. NEIHEISEL denied using or possessing any other device to access, store, or trade child pornography other than the tablet that was already in my custody since April 11, 2017. Upon conclusion of the consensual interview, NEIHEISEL departed to return to work.

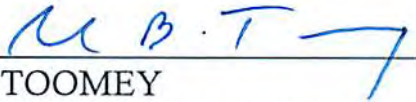
11. Based upon the foregoing facts, I have probable cause to believe that on or about February 7, 2016, at Jacksonville, in the Middle District of Florida, defendant, JASON JAMES NEIHEISEL, did knowingly distribute a visual depiction using any means and facility of interstate and foreign commerce by 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 depiction was of such conduct, the visual depiction being specifically identified in the computer file titled "bathtime with daddy-3yo girl ped.mpg", in violation of Title 18, United States Code, Section 2252(a)(2).



NICHOLAS PRIVETTE, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this  
3<sup>rd</sup> day of May, 2017, at Jacksonville, Florida.



JOEL B. TOOMEY  
United States Magistrate Judge

## UNITED STATES DISTRICT COURT

for the  
Middle District of FloridaCERTIFIED A TRUE COPY  
SHERYL L. LOESCH, CLERK  
U.S. DISTRICT COURT  
By: [Signature]  
Deputy Clerk

In the Matter of the Search of  
*(Briefly describe the property to be searched  
 or identify the person by name and address)*  
 a silver Microsoft Surface tablet,  
 with no visible serial number,  
 more particularly described in Attachment A

Case No. 3:17-mj-1101-POB

## 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)*:

The Evidence Control Room of the Jacksonville Field Office of the FBI, located at 6061 Gate Parkway, Jacksonville, Florida 32256,

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

a silver Microsoft Surface tablet, with no visible serial number, more particularly described in Attachment A.

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.

[Signature]  
 Nicholas Privette  
 Jonathan S. MacDonald, Special Agent, FBI  
 [Signature]  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 4/13/2017

City and state: Jacksonville, Florida

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

Exhibit A

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, Nicholas Privette, being duly sworn, state as follows:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since August 2016 when I began my law enforcement training at the FBI Academy in Quantico, Virginia. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes. Prior to this assignment, I was employed with the United States Army for approximately 12 years as an Infantry Officer and most recently held the position of Company Commander. I have a Bachelor of Science degree in Information Engineering and a Master of Science degree in Organizational Leadership. Since becoming a Special Agent, I have worked with experienced Special Agents, as well as other law enforcement officers and personnel, who investigate Child Exploitation offenses and other crimes against children. A substantial portion of my duties are dedicated to investigating and assisting with cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. In the performance of my duties, I have assisted in the investigation of matters involving the possession, collection, production, advertisement, receipt, and/or transportation of images of child pornography. I have been involved in searches of residences pertaining to the advertisement for, possession, collection, production, and/or transportation of child pornography

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

2. I have assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2252 and 2252A, as well as Florida state statutes which criminalize the possession, receipt, and transmission of child pornography, that is, visual images depicting minors engaged in sexually explicit conduct. In connection with such investigations, I have conducted interviews of subjects, witnesses, and victims, and I have observed experienced Special Agents serve in the role of case agent. I am a member of the FBI Jacksonville Field Office's Child Exploitation Task Force, comprised of federal, state, and local law enforcement agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on my personal knowledge, as well as on information provided to me by experienced Special Agents and other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of 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 a



violation of Title 18, United States Code, Section 2252 is present in the item 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 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)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed

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

e. The internet is a facility of interstate commerce.

#### **DEFINITIONS**

5. The following definitions apply to this Affidavit:

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

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct

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

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

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

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

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

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

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

compact discs, electronic or magnetic storage devices such as floppy diskettes, hard 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.

### **COMPUTERS AND CHILD PORNOGRAPHY**

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

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

8. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread

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

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

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

---

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

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 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<sup>2</sup>, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

---

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

### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

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

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

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



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

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

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

were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

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

15. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with

law enforcement officials. For example, I am familiar with the facts of an investigation conducted in the Middle District of Florida. In this investigation, 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. Based on my training and experience, as well as conversations with experienced law enforcement officers and computer forensic examiners, 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 through the use of forensic tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favored images involving a particular child or act is often maintained on the device.

**PEER-TO-PEER (P2P) FILE  
SHARING AND SHA-1 VALUE FILE IDENTIFICATION**

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

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

µTorrent client program, the Vuze client program, and the BitComet client program, among others.

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

19. Files or sets of files are shared on the BitTorrent network through the use of "Torrents." A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but rather contain information about the file(s) to be shared. This information includes the "info hash," which is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent. The term SHA-1 is a shorthand term for the hash value calculated by the Secure Hash Algorithm. The Secure Hash

Algorithm (SHA-1) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA-1 hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA-1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA-1 signature are identical copies of the same file regardless of their file names. The data contained in the Torrent information includes the SHA-1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This "info hash" uniquely identifies the Torrent file on the BitTorrent network.

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



then process that Torrent file to help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the Torrent file.

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

22. Law enforcement can search the BitTorrent network in order to locate individuals sharing child pornography images, which have been previously identified as such based on their SHA-1 values. Law enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a

single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

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

24. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. The ICAC Task Force Program uses law enforcement tools to track IP addresses suspected (based on SHA1 values and file names) of trading child pornography. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of whom were also involved in contact sexual offenses against child victims.

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

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

26. I make this affidavit in support of a search warrant for a silver-colored Microsoft Surface computer tablet, with no visible serial number, that was seized from Jason James Neiheisel at his residence located at [REDACTED], Jacksonville, Florida [REDACTED] on April 11, 2017 by me and FBI SA Jonathan MacDonald. This item is currently stored and secured in the FBI Jacksonville Field Office located at 6061 Gate Parkway, Jacksonville, Florida 32256.

27. The FBI is investigating Neiheisel as a suspect for using this Microsoft Surface tablet to commit violations of Title 18, United States Code, Sections 2252 and 2252A, which prohibit mailing, transportation, shipment, receipt, possession and access with intent to view, in interstate or foreign commerce by any means, including

by computer, any child pornography, that is, visual depictions of one or more minors engaging in sexually explicit conduct.

28. FBI Task Force Officer (TFO) Jimmy Watson has advised and provided SA Jonathan MacDonald and SA Abbigail Beccaccio with the following information, some of which was set forth in written documentation that I have reviewed. Along with my review of this information, I have also had conversations with SA MacDonald and SA Beccaccio regarding the origins and activities related to this investigation of Neiheisel. Based on my review and conversations, I know the following to be true:

a. On December 6, 2015, TFO Watson began an undercover operation to identify persons using the BitTorrent P2P network on the Internet to receive, traffic in, share and/or distribute images and videos depicting child pornography. I know that TFO Watson has received training in the operation and use of the BitTorrent P2P network, as well as certain law enforcement techniques used to investigate users on this network. TFO Watson was investigating host computers located in Florida that were actively sharing child pornography on the BitTorrent network. Through the use of specialized law enforcement software, TFO Watson was able to determine that a host computer using IP address 76.106.190.147 was associated with certain Files of Interest (FOI) by investigators conducting keyword searches or info hash value searches for files related to known child pornography images and videos.

b. Between February 6, 2016 at 03:51 Eastern Standard Time (EST) and February 7, 2016 at 03:56 EST, a law enforcement computer used and controlled by TFO Watson made a successful connection to a host computer at IP address 76.106.190.147 using an undercover computer through the internet. Using this connection and specialized software, this law enforcement computer successfully downloaded 1,575 pieces of a total of 7,702 pieces of a video collection from the host computer at IP address 76.106.190.147, and through this connection it was confirmed that this host computer possessed 7,653 pieces. Included in these 1,575 pieces were approximately 56 viewable videos, of which two particular videos with the title "bathtime with daddy-3yo girl ped.mpg" and a title with several foreign characters and the words "R@ygold", "Lolita", and "Bed Sex", are further described below. I know the above information based on conversations with experienced Special Agents and other personnel, and my review of TFO Watson's investigative reports, including the log file report of the undercover session which was submitted into the FBI's case file management system.

29. Regarding my conversations with SA Beccaccio and SA MacDonald and thorough review of all historic information and investigative activity related to this case, I know the following information to be true:

a. Through the use of Arin, a publicly available online resource, the IP address 76.106.190.147 was determined to be issued to Comcast Communications.

b. At the request of SA Beccaccio, on June 14, 2016, FBI Operational Support Technician (OST) James Guy prepared an administrative subpoena (number 310130) directed to Comcast Communications requesting the subscriber and billing information for the account associated with IP address 76.106.190.147 for the dates and times of December 6, 2015 at 03:35 EST, December 15, 2015 at 17:27 EST, and February 7, 2016 at 11:04 EST.

c. On June 16, 2016, the Comcast Legal Response Center responded to this administrative subpoena and provided the following information that I have reviewed. The subscriber information for the IP address 76.106.190.147 during the dates and times listed above resolved back to account number 8495741212254787, registered to Jason Neiheisel, [REDACTED] Jacksonville, Florida [REDACTED]. The email addresses associated with this account were neijeijj@comcast.net and [REDACTED].

d. At the request of SA Beccaccio, on July 12, 2016, FBI Staff Operations Specialist (SOS) Lucy Spagnuolo conducted a query of the Florida Drivers and Vehicle Information Database (DAVID) for persons holding a State of Florida Driver's License or Identification Card residing at [REDACTED] Jacksonville, Florida [REDACTED]. This query revealed Florida driver's licenses issued to the following persons residing at this address: JASON JAMES NEIHEISEL (date of birth XX/XX/1990) and [REDACTED] (date of birth [REDACTED]).

30. Regarding my personal involvement in this investigation, in conjunction with my review of historic information and conversations with SA Beccaccio and SA MacDonald, I know the following to be true:

a. On April 5, 2017, I conducted a Florida DAVID query for Jason James Neiheisel and confirmed the same address of [REDACTED] Jacksonville, Florida [REDACTED]. This query also revealed that a gray 2014 Dodge utility vehicle with Florida license plate 60NFX was currently registered to Neiheisel.

b. On April 5, 2017, SA Joseph Barriere and I conducted physical surveillance at the residence located at [REDACTED] Jacksonville, Florida [REDACTED]. We learned that the address is part of the [REDACTED] Apartments complex and observed that a vehicle matching the description above was parked in the vicinity of building 4. The vehicle was a dark gray Dodge Durango with Florida license plate 60NFX. I walked into building 4 and confirmed that apartment number [REDACTED] was on the first floor in the eastern-most portion of the building.

c. On April 10, 2017, SA MacDonald and I reviewed several viewable portions of the approximately 56 videos mentioned above in paragraph 28.b. that TFO Watson caused to be downloaded from the host computer connected to the Internet through IP address 76.106.190.147 between February 6, 2016 at 03:51 EST and February 7, 2016 at 03:56 EST. Included in the 1,575 pieces, as mentioned in paragraph 28.b/, are two videos with the title "bathtime with daddy-3yo girl ped.mpg" (hereafter Video 1), and a title with several foreign characters and the

words "R@ygold", "Lolita", and "Bed Sex" (hereafter video 2). The contents of these videos are further described below:

(1) Based on my training and experience, as well as conversations with experienced Special Agents and law enforcement officers, I believe that Video 1 (more fully described below) depicts at least one minor engaged in sexually explicit conduct (oral to genital sexual intercourse, or fellatio), and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256. As described herein, the SHA-1 values for this video are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). Video 1, which TFO Watson caused to be downloaded from IP address 76.106.190.147 between February 6, 2016 at 03:51 EST and February 7, 2016 at 03:56 EST, that was being offered for sharing on the date and times listed below, is described as follows:

SHA-1: 4f03620ae4fb255ba98d6ba5651e2d762f19977f

DATE: February 7, 2016 at 3:56:47 a.m. EST

TITLE: bathtime with daddy-3yo girl ped.mpg

DESCRIPTION: This is a color video of 3:25 (minutes:seconds) duration, of which the entirety was downloaded directly from a host computer at IP address 76.106.190.147. I have reviewed this video. This video depicts what appears to be a 3 to 4 year-old female seen naked in a bathtub. The video has sound and a man can be heard speaking to this minor child, who is standing naked in the bathtub



and spreading open her genitals. A male asks the female girl, "Can you rub it?" as she is spreading open her genitals. At 1:56, this prepubescent child is then seen with her hands on an adult male's erect penis. At 2:10, this child places this erect penis in her mouth. The male is seen with his hand on the back of this child's head, pulling her head and mouth onto his erect penis. The activity continues through the end of the video.

(2) Based on my training and experience, as well as conversations with experienced Special Agents and law enforcement officers, I believe that Video 2 depicts at least one minor engaged in sexually explicit conduct (oral to genital sexual intercourse, or fellatio), and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256. As described herein, the SHA-1 values for this video are contained on the list of those known or designated as a FOI depicting images of child pornography. These SHA-1 values are catalogued by the Internet Crimes Against Children Task Force (ICAC). Video 2, which TFO Watson caused to be downloaded from IP address 76.106.190.147 between February 6, 2016 at 03:51 EST and February 7, 2016 at 03:56 EST, that was being offered for sharing on the date and times listed below, is described as follows:

SHA-1: aa5241853c63b69c3f71ebf1b9d2a75115a37acf

DATE: February 7, 2016 at 3:56:42 a.m. EST

TITLE: several foreign characters and the words "R@ygold",  
"Lolita", and "Bed Sex".mpg

DESCRIPTION: Video 2 is a color video of 10:26 (minutes:seconds) duration, of which the entirety was downloaded directly from a host computer at IP address 76.106.190.147. I have reviewed this video. This video depicts what appears to be a 5 to 7 year-old female child performing oral sex on an adult male. At 1:47, this prepubescent girl is lying on the bed with no pants on and exposing her genitals. Then the girl begins to masturbate. At 5:00, the girl is again shown performing oral sex on an adult male. The activity continues through the end of the video.

d. On the evening of April 10, 2017, I conducted physical surveillance of the residence located at [REDACTED] Jacksonville, Florida [REDACTED] and observed the same vehicle listed above in paragraph 30.b. parked in the same location in the vicinity of building 4.

31. On April 11, 2017, SA MacDonald and I conducted a consensual interview of Jason James Neiheisel at his residence located at [REDACTED] Jacksonville, Florida [REDACTED]. Hall answered the door and invited us inside the residence. Moments later, Neiheisel emerged from a different room and joined us. After being advised of our identity and the general nature of the investigation, Neiheisel agreed to speak with us in his residence and provided the following information:

a. Neiheisel and [REDACTED] <sup>WP</sup> [REDACTED] moved into their current apartment in or around October of 2015.

b. Neiheisel only knows the neighbors through casual passage in the hallways, and they do not socialize together. During the time Neiheisel and [REDACTED] lived in the apartment, they had occasional visitors of family and friends, none of whom stayed longer than four or five days. Neiheisel and [REDACTED] have never had any other roommate.

c. Neiheisel has Comcast Internet service at the apartment in Neiheisel's name, and the wireless service is password protected. Neiheisel set up the password protected network with a router he had from before. Neiheisel has a solid understanding of information technology and knew his home network was secured, and he and [REDACTED] did not share their password with neighbors or others. They do provide the password to the network to family and friends who visit; however, never to strangers.

d. Neiheisel has two laptop computers in the residence - a work laptop and a personal Microsoft Surface tablet. The work laptop was sitting on the couch next to Neiheisel, and the Surface tablet was in a different room that Neiheisel retrieved to show to me and SA MacDonald. Neiheisel placed the Surface tablet on the coffee table in front of me and SA MacDonald where the interview was taking place. Both devices are password protected, and the work laptop has an RSA SecureID token as part of its security. He has owned the Surface tablet since before 2015 and uses it at this current address to access the Internet.

e. Neiheisel used the personal tablet for downloading movies such as "Elf" which he watches on flights to Cincinnati. He was familiar with file sharing

programs including Limewire and BitTorrent but was unsure if he had BitTorrent currently installed on his Surface tablet. Neiheisel picked up the Surface tablet, pushed a few keys, and advised that the BitTorrent program was not on the Surface tablet. SA MacDonald and I were unable to observe the screen of the Surface tablet when Neiheisel did this.

f. Neiheisel had downloaded child pornography for “a while” and last did so within the past two months. Neiheisel knows child pornography is illegal and has viewed and downloaded child pornography with his Surface tablet. I showed Neiheisel a screen print of several files of child pornography downloaded from the IP address at Neiheisel’s apartment. Neiheisel read some of the file titles and recognized them as ones he downloaded. He also knew the terms “PTHC” and “YO” as child pornography related terms but did “not want to say” what they stood for. SA MacDonald and I asked for clarification, and Neiheisel stated he was “not comfortable saying” the long form of the abbreviations.

g. Neiheisel had seen child pornography “by accident” and later clarified that he gets his child pornography through a chat room called “Chat Tango.” Neiheisel did not need to use search terms to find child pornography because the chat room he accessed had users who provided various links that took him to child pornography content.

h. SA MacDonald showed Neiheisel a video of child pornography downloaded from Neiheisel’s IP address at his residence titled, “bathtime with daddy-3yo girl ped.mpg” (previously described above as Video 1), which depicted a

prepubescent female child being sexually abused by an adult male. Neiheisel recognized the video as one he downloaded and viewed but denied masturbating to the video. Neiheisel downloaded that particular video within the past week and confirmed he used the Surface tablet that was sitting on the coffee table to download and view the video.

i. SA MacDonald also showed Neiheisel a video with a title containing several foreign characters and the words "R@ygold", "Lolita", and "Bed Sex" (as previously described above as Video 2), which depicted a prepubescent female child being sexually abused by an adult male. Neiheisel also recognized the video as one that he had downloaded and viewed and confirmed he used the Surface tablet that was sitting on the coffee table to download and view the video.

j. Neiheisel downloaded child pornography for "personal use" in the privacy of his bedroom. No one else knows about his child pornography activities, including [REDACTED] Neiheisel denied that child pornography would be found on the Surface tablet saying "there shouldn't be" any child pornography saved on the tablet.

k. Using a variety of means to download child pornography, Neiheisel understood child pornography is saved to his "downloads" folder and in the past, he has organized and categorized his child pornography videos. Neiheisel noted that he downloaded child pornography to "see if I can find it" and indicated he is able to find other "files like that you'll find" in reference to the ones shown to him by me and SA MacDonald. Neiheisel also noted that he enjoyed the "thrill of the

hunt” to see what kind of child pornography files he could find, such as the age range or level of explicit content.

1. Neiheisel was asked for consent to search his Surface tablet and was advised that he did not have to provide consent. Neiheisel stated that he was interested in cooperating with me and SA MacDonald but did not feel comfortable providing consent at the time. Neiheisel did provide the password to the Surface tablet as “strange777” and told me and SA MacDonald that he needed to leave for work.

32. Upon conclusion of the consensual interview, SA MacDonald and I advised Neiheisel that we were securing the Surface tablet based on his statements about it being used to download child pornography. As stated above, this Surface tablet was within our plain view and Neiheisel had referred to it as set forth above. I provided Neiheisel with a FD-597 Receipt for Property Received form, describing the item, which Neiheisel and I both signed. Neiheisel believed that SA MacDonald and I had treated him fairly, and he understood the importance of our investigation.

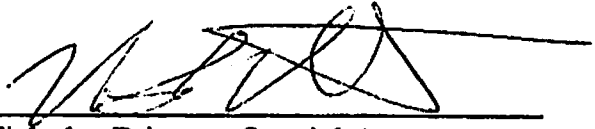
### CONCLUSION

33. Based on the foregoing, I have probable cause to believe that fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including images and/or videos of child pornography, are currently contained in the item listed and described above, that is, the silver-colored Microsoft Surface computer tablet, with no visible serial number, that was seized


from Jason James Neiheisel at his residence located at [REDACTED]

[REDACTED] Jacksonville, Florida [REDACTED] on April 11, 2017.

34. Accordingly, I respectfully request a search warrant be issued by this Court authorizing the search and forensic examination of the item listed in Attachment A, for evidence as set forth in Attachment B.

  
\_\_\_\_\_  
Nicholas Privette, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this  
13<sup>th</sup> day of April, 2017, at Jacksonville, Florida.

  
\_\_\_\_\_  
PATRICIA D. BARKSDALE  
United States Magistrate Judge

**ATTACHMENT B**  
**LIST OF ITEMS TO BE SEIZED AND SEARCHED**

1. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs, including, but not limited to, P2P 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 produce, distribute, possess or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs and electronic messages) pertaining to the production, possession, receipt, or distribution of child pornography as defined in 18 U.S.C. Section 2256(8) or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. Section 2256(2).
3. In any format and medium, all originals, files, and copies of images and/or videos depicting child pornography as defined in 18 U.S.C. Section 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. Section 2256(2), or child erotica.
4. 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 device or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. Section 2256(2).
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. Section 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256(2).
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning



the production, receipt, transmission, or possession of child pornography as defined in 18 U.S.C. Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of websites or file sharing networks on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail 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.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, 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.

11. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, images, videos, e-mail messages, chat logs and electronic messages, and other digital data files), which show the identity of the users of any of the electronic storage media described herein.

12. Any and all diaries, notes, e-mail messages, chat logs and electronic messages, other digital data files reflecting personal contact with minors, sexual activity with minors, and/or any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256(2).

**ATTACHMENT A**  
**ITEM TO BE SEARCHED**

The item to be searched is described as follows:

A silver-colored Microsoft Surface computer tablet, with no visible serial number, that was seized from Jason James Neiheisel at his residence located at [REDACTED] Jacksonville, Florida [REDACTED] on April 11, 2017.

The above-described item was seized from NEIHEISEL during his consensual interview on April 11, 2017, and is currently secured in the Jacksonville Division of the Federal Bureau of Investigation, 6061 Gate Parkway, Jacksonville, Florida 32256.