

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

Sealed~~Public and unofficial staff access
to this instrument are
prohibited by court order.~~

UNITED STATES DISTRICT COURT

for the
Southern District of TexasUnited States Courts
Southern District of Texas
FILED

MAR 18 2014

David J. Bradley, Clerk of Court

Unsealed per 3/19/2014 order

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)One SanDisk Cruzer USB Flash Drive
Located at One Justice Park Drive, Houston, Texas
77092Case No. **H14-278 MJ**

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):

One SanDisk Cruzer USB flash drive, 16GB, black and red, with number BL13052, further described in Attachment A, located in the Southern District of Texas, 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
Title 18 USC § 2251	Production of Child Pornography
Title 18 USC § 2423(b) and (c)	Illicit Sexual Activity in a Foreign Country

The application is based on these facts:

- ☒ 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.

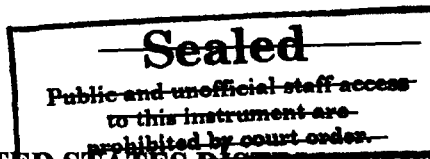

 Applicant's signature
Michael T. Whitmire, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: March 19, 2014

 Judge's signature
City and state: Houston, TexasStephen W. Smith, U.S. Magistrate Judge
Printed name and title

SLZ 3/18/14



Unsealed per 3/19/2014 order

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS**

**IN THE MATTER OF THE SEARCH OF
ONE SANDISK CRUZER USB FLASH DRIVE
CURRENTLY LOCATED AT ONE JUSTICE
PARK DRIVE, HOUSTON, TEXAS 77092**

:
:
: **H14-278 MJ**
:

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michael T. Whitmire, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

A. Introduction and Agent Background:

1. I have been employed as a Special Agent of the FBI since January 2005. I am currently assigned to the FBI's Innocent Images Operations Unit in Linthicum, Maryland. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography.
2. I attended the 22nd annual Crimes Against Children Conference in Dallas, Texas and completed classes related to the online sexual exploitation of children. I have also completed numerous classes related to the investigations of cyber crimes and child pornography.
3. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

B. FACTS AND CIRCUMSTANCES:

4. The statements in this affidavit are based on my personal observations, my training and experience, my investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2423(b) and (c) are present in the electronic devices described in this affidavit.

5. I make this affidavit in support of an application for a search warrant for one red and black SanDisk Cruzer Glide 16GB USB flash drive, identified with number BL13052 (hereafter referred to as the “electronic evidence”). The electronic evidence is currently located in the offices of the FBI at One Justice Park Drive, Houston, Texas, 77092 and is further described in the following paragraphs and in Attachments A and B.

6. I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, involving the use of a computer in or affecting interstate commerce to produce child pornography, is located in and within the aforementioned electronic evidence. I also have probable cause to believe that evidence of violations of 18 U.S.C. §§2423(b) and (c) involving the engaging of illicit sexual activity while traveling to or from, or residing in, a foreign nation is located within the electronic evidence. Additionally, I have probable cause to believe that the electronic evidence contains evidence regarding the possible locations and identities of minors depicted in various images, including images depicting minors engaged in sexually explicit conduct.

C. STATUTORY AUTHORITY

7. This investigation concerns alleged violations of Title 18, United States Code, §§2251, 2423(b) and 2423(c):
- a. 18 U.S.C. § 2423(b) prohibits a United States citizen or alien admitted for permanent residency from knowingly traveling in foreign commerce for the purpose of illicit sexual conduct with another person.
 - b. 18 U.S.C. § 2423(c) prohibits a United States citizen or alien admitted for permanent residency from knowingly traveling in foreign commerce or residing in a foreign country and engaging in illicit sexual conduct with another person.
 - c. 18 U.S.C. §2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for purpose of transmitting a live visual depiction of such conduct.

D. DEFINITIONS:

8. The following definitions apply to this Affidavit and its Attachments
- a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
 - b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as 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 areas of any person.

- c. The phrase “illicit sexual conduct” means a sexual act (as defined in section 2246) with a person under 18 years of age; or any commercial sex act (as defined in section 1591) with a person under 18 years of age. *See* 18 U.S.C. § 2423(f).
- d. Title 18, United States Code, Section 2246(2) defines “sexual act” as:
 - (A) contact between the penis and the vulva or the penis and the anus, which occurs upon penetration, however slight; (B) contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus; (C) the penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person; or (D) the intentional touching, not through the clothing, of the genitalia of another person, who has not attained the age of 16 years with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person.
- e. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other 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 a permanent format.
- f. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage

facility or communications facility directly related to or operating in conjunction with such device.

g. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

- h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique 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. A creation IP address is the address used on the date that an e-mail account is created by the user.
- i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.
- j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- k. A “Preservation Letter” is a letter governmental entities may issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in its possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.
- l. The term “child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but are not, in

and of themselves, obscene and do not necessarily depict minors in sexually explicit poses or positions.

E. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND EMAIL:

9. I have had both training and experience in the investigation of computer-related crimes.

Based on my training, experience and knowledge, I know the following:

- a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.
- b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

- c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.¹ Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.
- e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

¹ The File Transfer Protocol (FTP) is a protocol that defines how to transfer files from one computer to another. One example, known as “anonymous FTP,” allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

- f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Microsoft Corporation, Yahoo! and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail 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. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
- g. As is the case with most digital technology, communications 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 e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information 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). 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 peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

G. BACKGROUND OF THE INVESTIGATION:

10. On approximately March 14, 2014, FBI agents in Houston, Texas telephonically interviewed an employee of the American Nicaraguan School, located in Pista Suburbana, Managua, Nicaragua.

11. William James Vahey (hereafter after referred to as "Vahey"), was hired in June of 2013 to teach ninth grade world history and advanced geography at this school. He signed a two year contract on July 1, 2013, and started teaching on August 12, 2013. Vahey is a United States citizen.

12. The investigation has revealed two residences for Vahey. The first address, 28C Maida Avenue, Paddington W2-First, London, United Kingdom, is the current residence of Vahey's wife. The second address, 8 Greenwing Teal Road, Hilton Head Island, South Carolina, 29929, was used by Vahey as his United States home address on his job application for the American School. Subsequent investigation revealed Vahey's home address on his South Carolina Department of Motor Vehicles records to be: 8 Green Wing Teal Road, Hilton Head Island, South Carolina, 29928.

13. In November, 2013, Vahey reported a theft of personal items from his apartment to employees at the American Nicaraguan School. The only other person who had access to Vahey's apartment was a maid, who was hired and paid by the American Nicaraguan School to clean Vahey's apartment. After Vahey notified the school of the theft, the maid was immediately terminated.

14. On March 11, 2014, Vahey's former maid brought a USB thumb drive to the American Nicaraguan School. She admitted to taking the thumb drive from Vahey's home and to viewing

its contents. The former maid indicated to employees at the school that she was giving them the thumb drive due to some of the contents she had seen.

15. An employee of the American Nicaraguan School conducted a cursory review of the contents of the flash drive, initially reviewing the menu of the flash drive. The menu consisted of several folders titled with locations and corresponding dates/years, including: "Panama Trip," "Costa Rica Trip," and "Basketball Trip." The School employee observed a folder titled "Spring 2013." The employee opened this folder and viewed the contents, which included several images.

16. According to the employee, these images depict minor males, in various states of undress. In some of the images, the minors' genital or pubic area is exposed. The minor males appear to be asleep, unconscious or possibly drugged. The minor males appear to be middle-school aged, which would be approximately 12 to 14 years of age. Some of the images depict minor males posed with their penises placed into the mouths of other minor males. Furthermore, several images depict the anuses/rectums and testicles of various individuals. The underage males had blond and red hair, ruddy cheeks and pale skin. In some of these images, what appears to be an adult male's hand is seen touching the minors' testicles and anuses and fondling their bodies. No jewelry was observed on the hands depicted in these images; however, the School employee believed the adult male hands depicted in these images to be Vahey's.

17. According to the American Nicaraguan School employee, the folder names viewed on the menu page of the flash drive matched locations where Vahey previously traveled with students.

18. After viewing these images, the School employee confronted Vahey about the contents she had viewed on the thumb drive. In response, Vahey stated in sum and substance, "I was molested as a boy, that is why I do this. I have been doing this my whole life". Vahey further

stated he "never hurt any of the boys" and that "they did not know what had happened to them; they were completely asleep." The School employee asked Vahey if he had given the minors "date rape drugs." In response, Vahey replied, "No, I used sleeping pills".

19. The School employee demanded Vahey's resignation. The next day, Vahey left Nicaragua on a flight to Atlanta, Georgia, connecting through Miami, Florida. On March 12, 2014, Vahey was on American Airlines flight 344 from Managua, Nicaragua to Miami, Florida. Vahey was scheduled to take American Eagle flight 3512 from Miami, Florida to Atlanta, Georgia the following day. The school employee notified the Regional Security Office (RSO) at the United States Embassy in Managua, Nicaragua. The RSO notified the FBI Legal Attache office in the Embassy, who notified FBI in Houston, Texas.

20. The USB flash drive removed from Vahey's home by the former maid (described fully in paragraph 5) was given by the school to the RSO office in Managua, Nicaragua, who then gave the flash drive to the FBI's Legal Attache office in Nicaragua. The drive was then transported by FBI agents from Managua, Nicaragua, to the FBI office in Houston, Texas, where it is currently located. The electronic evidence has not been accessed or reviewed to date.

H. CHARACTERISTICS OF PERSONS WHO COMMIT SEX OFFENSES AGAINST MINORS AND THOSE INVOLVED IN THE PRODUCTION OF CHILD PORNOGRAPHY:

21. A review of court documents received from a Criminal Intelligence Specialist with the California Department of Justice, Sex Offender Tracking Program, located at 4949 Broadway, Room H216, Sacramento, California, 95820 revealed that Vahey was arrested in 1969 on six

counts of violating California Penal Code 288, Child Molestation. He pled guilty to one count on January 22, 1970 and was sentenced to 90 days in jail and five years' probation. Criminal records indicate that, at the time, Vahey worked with minors as a swim instructor. It is alleged that he fondled the minor males' genitals or pubic areas with his hand, both over and under their clothing. As a result of this conviction, Vahey is required to register in the State of California Sex Offender Registry for the remainder of his life. A review of relevant records indicates that while Vahey registered as a Sex Offender once in 1970, he has not renewed his registration since.

22. Based on my training and experience, individuals who commit sex offenses involving children often use digital cameras and other recording devices to photograph or film their victims and the sexual contact that they engage in with these children. Cellular telephones with camera functionality and digital cameras are often used by these individuals to produce child pornography which can be easily uploaded onto a computer, other items of digital media, and the internet, and distributed to others with a sexual interest in minors.

23. Based on my training, knowledge and experience, I am aware that individuals who commit sex offenses involving minors will often collect and/or view child pornography on their computer for several reasons:

- a) They will receive sexual gratification and satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or sexually suggestive poses;
- b) They collect sexually explicit or sexually suggestive materials in a variety of media that they use for their own sexual arousal and/or gratification;

c) They almost always possess and maintain their material in the privacy and security of their homes or some other secure location. Child pornography distributors/collectors typically retain recordings, mailing lists, child erotica and videos for many years and store their child pornography amongst other, otherwise legal media or files. Digital evidence, like child pornography contraband, is different than traditional evidence that can be concealed, sold, used and/or destroyed and is not as volatile as other illegal items like narcotics.

d) Likewise, those who produce, distribute, receive or possess child pornography, or who attempt to commit these crimes, often maintain their collections in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

I: REQUEST TO SEARCH THE ELECTRONIC EVIDENCE

24. In light of the foregoing information, and based on my experience and training, I submit that there is probable cause to believe that the electronic evidence contains child pornography or other evidence concerning violations of Title 18 United States Code, Section 2423(b) and (c); Traveling with the Intent to Engage in and Engaging in Illicit Sexual Conduct in Foreign Places and that the fruits and instrumentalities of those violations can be found in the electronic evidence.

**J. METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS AND
COMPUTER-RELATED EQUIPMENT LOCATED IN THE PREMISES:**

25. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers and other electronic media, I know that electronic data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve data from the system or phone in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is

essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. A terabyte of storage space has the capacity to store 100,000 times that amount of text. Storage devices capable of storing up to 1 Terabyte of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of millions of pages of data.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

26. The analysis of electronically stored data may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); “opening” or reading the first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “key-word” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

27. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the offense specified above.

28. In searching the data, the computer personnel may examine all of the data contained in the cell phones, computers, computer equipment and storage devices, including the electronic evidence, to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit.

29. The hard drive has the capability of copying information from the computer to DVD/CD-rom discs or to USB thumb drives, and to store data extracted from the camera memory card. The hard drive also has the ability to read and write directly to the memory card.

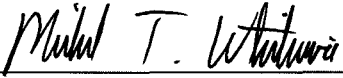
30. Based on the foregoing, there is probable cause to believe that the items described in Attachment B, which is incorporated by reference as if set out fully herein, contain evidence of the commission of said criminal offense, or are property which is or has been used as the means of committing said criminal offenses.

K. CONCLUSION:

31. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the electronic evidence there exists evidence of a crime, contraband and/or fruits of a crime, and evidence leading to the identification of the individual responsible for the crimes described above. Accordingly, a search warrant is requested.

32. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A)

& (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(I). Furthermore, the electronic evidence to be searched is located within this Court’s jurisdiction.



Michael T. Whitmire

Special Agent

Federal Bureau of Investigation

Subscribed and sworn before me this 19th day of March 2014.



Stephen W. Smith

United States Magistrate Judge

Southern District of Texas

ATTACHMENT A

ITEMS TO BE SEARCHED

This warrant applies to the electronic evidence currently located in the FBI office building at

One Justice Park Drive, Houston, Texas, 77092. This device is described as:

One red and black SanDisk Cruzer Glide 16GB USB flash drive, identified with number
BL13052.

ATTACHMENT B

Particular Things to be Seized

A. All electronic data, including image files, graphic interchange formats, and other visual depictions of minors, including minors engaging in sexually explicit conduct, as that term is defined in Title 18, United States Code, Section 2256(2); any data that contains information pertaining to a sexual interest in children, child pornography or pertaining to sexual activity with children; or which indicates the distribution, possession, or receipt of child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica; including, but not limited to, .jpg files, .gif files, .tif files, .avi files, and .mpeg files; or any other video images in any form and format.

B. All other records, documents, electronic communications and items relating to the production of child pornography for importation into the United States or traveling in interstate or foreign commerce and/or travel with the intent to engage in or engaging in illicit sexual conduct, constituting evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251(c) and 2423(b) and (c).

C. 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, and other digital data files) pertaining to travel in interstate or foreign commerce and/or traveling with the intent to engage in and/or engaging in illicit sexual conduct in foreign places.

D. 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, and other digital data files) pertaining to the production, possession, receipt, transmission,

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

E. Any and all diaries, address books, names, and lists of names and addresses of individuals, in any format and medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files), who may have been contacted by the operator of the Computer described in Attachment A for the purpose of child sex tourism, sex tourism, and/or producing, distributing, receiving or possessing 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).

F. 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), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the U.S. Mail or by 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).

G. 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 sites on the Internet that contain child pornography or that cater to those with an interest in child pornography and/or traveling with the intent to engage in and/or engaging in illicit sexual conduct in foreign places.

H. 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, and/or that advertise, promote, discuss or otherwise involve traveling with the intent to engage in and/or engaging in illicit sexual conduct in foreign places.

I. Any and all travel 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).

J. 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 image creation information, online storage or other remote computer storage information, 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.

K. Any and all visual depictions of minors.

L. Any and all 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), pertaining to occupancy or ownership of the items to be searched described above, including, but not limited to, billing, account status, or electronic receipts.