AFFIDAVIT

STATE OF WASHINGTON ss

COUNTY OF PIERCE

I, Douglas Shook, being first duly sworn on oath, depose and say:

INTRODUCTION

1. I have been employed as a Task Force Officer of the FBI since May 2015, and am currently assigned to the Child Exploitation Task Force (CETF). While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber-crime, child exploitation, and child pornography. I have gained experience through previous law enforcement training and investigations, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. I have been an employee of the Pierce County Sheriff's Department since August of 2000. I began my employment as a Corrections Officer at the county jail. While there, I worked many positions including inmate housing supervision, booking officer, court escort, internal escort, and hospital transport. I transferred to the patrol division in April 2003. I have worked in the contract cities of Lakewood and University Place on assignment. I have also worked in the Foothills Detachment (D12), Mountain Detachment (D10), Courts (City County Building), and East Side Patrol (South Hill Precinct). In 2005, I transferred to University Place Detachment. While in University Place, I worked all three shifts, served 3 years as the School Resource Officer, and three years as the Investigator. I was assigned to the PCSD CID Special Assaults Unit from November 2013 to February 2014. I worked as the supervising Deputy of the Pierce

County Superior Court Alternatives to Confinement program from July 2014 to May 2015. I am currently assigned as one of the Task Force Officers assigned to the FBI in the South Sound Child Exploitation Task Force.

3. I have attended OJJDP Internet Crimes Against Children Investigative Techniques Training Program, OJJDP Responding to Missing and Abducted Children, Craigslist Investigations Class, Internet Profiling and Intelligence Gathering, School Resource Officer certification class (NASRO), the 2011 National District Attorneys Association Annual Multidisciplinary Conference on Domestic Violence, Investigating Stalking class, Mental Health Officer class, the Reid Interview and Interrogation class, Practical and Kinesthetic Interview and Interrogation class, Firearm Crimes Enforcement class, Criminal Street Gangs class, Gang Recognition and Psychology of Gangs class, Field Training Officer certification class, Insurance Fraud and Auto Theft Prevention training, Methamphetamine training class, and Emergency Response To Terrorism. I have also conducted Bait Vehicle Operations within the city of University Place

4. Moreover, I am a federal law enforcement task force officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

5. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2252(a)(2), (a)(4)(B) and (b)(2) (possession of, knowing access, receipt, or attempted access with intent to view child pornography), are located within 8522 20th St. Ct. W, University Place, WA 98466 (hereinafter the "SUBJECT PREMISES"), within the SUBJECT VEHICLES, and on the person of David W. Tipppens. I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, SUBJECT VEHICLES and the person of David W. Tippens, as further described in Attachment A for the items set forth in Attachment B, incorporated herein by reference, which is located in the Western District of Washington. Located within these locations to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I

request authority to search the locations described in Attachment A, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

6. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Task Force Officer with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

DEFINITIONS

7. The following definitions apply to this Affidavit and attachments hereto:

(a) "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private

messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

(b) "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

(c) "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, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

(d) "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as 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.

(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 or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

(f) "Computer Server" or "Server," as used herein is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the

Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

(g) "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).

(h) "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.

(i) "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

(j) "Computer passwords, pass-phrases 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 or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code 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 "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

(k) "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

(l) "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

(m) "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

(n) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

(o) "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a

personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

(p) "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access 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. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

(q) Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

(r) "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

(s) 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, painting), 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"), Multi Media 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).

(t) "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

(u) "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-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 person. See 18 U.S.C. § 2256(2).

(v) "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

(w) "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

(x) "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP");

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

8. David Tippens or another person residing at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child

pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as "Website A."[1] There is probable cause to believe that Tippens or another individual residing at the SUBJECT PREMISES knowingly possessed, received, or accessed with intent to view child pornography on "Website A."

THE NETWORK[2]

9. "Website A" operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.[3] Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

10. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A"

---

1 The actual name of "Website A" is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "Website A."

2 The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

3 Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

could not generally be accessed through the traditional Internet.[4] Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

11. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user.

12. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP

---

4 Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

DESCRIPTION OF "WEBSITE A" AND ITS CONTENT

13. The information covered in sections 14-36 were data provided by the master/core case investigators of the FBI. As the investigator/TFO for the candygirl123 case, I did not directly witness the site or the documented activity by "candygirl123."

14. "Website A" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting "Website A" was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

15. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. Between September of 2014 and February 19, 2015, on the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred,

encrypt filenames, include preview, Peace out."[5] Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

16. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

17. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

18. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional

---

[5] On February 19, 2015, the site administrator replaced those two images with a single image, located to the left of the site name, depicting a prepubescent female, wearing a short dress and black stockings, posed sitting reclined on a chair with her legs crossed, in a sexually suggestive manner, and the text "No cross-board reposts, .7z preferred, Encrypt filenames, Include preview," to the right of the image.

sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors; the abbreviation "HC" means hardcore (i.e., depictions of penetrative sexually explicit conduct); and "scat" refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

19. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The "last post" section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

20. A review of the various topics within the "[Website A] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

21. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

(a) On February 3, 2015, a user posted a topic entitled "Buratino-06" in the forum "Pre-teen – Videos - Girls HC" that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

(b) On January 30, 2015, a user posted a topic entitled "Sammy" in the forum "Pre-teen – Photos – Girls" that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and

(c) On September 16, 2014, a user posted a topic entitled "9yo Niece - Horse.mpg" in the "Pre-teen Videos - Girls HC" forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

22. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, "Website A" contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

23. "Website A" also included a feature referred to as "[Website A] Image Hosting." This feature of "Website A" allowed users of "Website A" to upload links to images of child pornography that are accessible to all registered users of "Website A." On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita" which was created by a particular "Website A" user. The post contained links to images stored on "[Website A] Image Hosting." The images depicted a prepubescent girl in various stages of undress. Some images were focused on the nude genitals of a

prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

24. Text sections of "Website A" provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse.

(a) On January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

COURT AUTHORIZED USE OF NETWORK INVESTIGATIVE TECHNIQUE

25. Websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

26. However, because of the Network software utilized by "Website A," any such logs of user activity would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such

communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of "Website A."

27. Accordingly, on February 20, 2015, the same date "Website A" was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A." Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

"candygirl123" ON "WEBSITE A"

28. According to data obtained from logs on "Website A," monitoring by law enforcement and the deployment of a NIT, a user with the user name "candygirl123" engaged in the following activity on "Website A."

29. The profile page of user "candygirl123" indicated this user originally registered an account on "Website A" on December 18, 2014. Profile information on

"Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user "candygirl123's" profile, this user was a NEWBIE Member of "Website A." Further, according to the Statistics section of this user's profile, the user "candygirl123" had been actively logged into the website for a total of 26 hours between the dates of December 2014 and March 2015.

30. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on February 28, 2015, the user "candygirl123" engaged in the following activity on "Website A" from IP address 66.8.138.192, utilizing MAC Address: F04DA2609893, Host Name: "bubba-pc," Log-On ID: "bubba." During the session described below, this user browsed "Website A" after logging into "Website A" with a username and a password.

31. On February 28, 2015, the user "candygirl123" with IP address 66.8.138.192 accessed the post titled, "Latina Anal Part 1 & 2." Among other things, this post contained links and download passwords to a video depicting a young toddler age girl as she was orally, anally, and vaginally penetrated by an adult male penis. The thread contained 38 thumbnail images as a preview of the video. These images were embedded in the post and thus visible to the user. I have viewed these images, and they depict a toddler being subjected to various sexual acts, including penetrative sex.

32. During the following additional sessions, the user "candygirl123" also browsed "Website A" after logging into "Website A" with a username and password. During these sessions, the user's IP address information was not collected.

33. On February 26, 2015, the user "candygirl123" accessed the post titled, "Re: Requested: 8yo fox", which was located in the "Pre-teen Photos", "Girls HC" section of "Website A". This post contained 2 embedded images, which I have viewed, that depicted a nude prepubescent female. In one image the prepubescent female is depicted sitting on a bed with her legs spread and her nude genitals exposed to the

camera. The second image depicts the nude prepubescent female with her hands "hogtied" together with a rope. The prepubescent female's nude genitals and anus are exposed to the camera. Based on the child victim's size, facial features, and physical development, I believe the child victim depicted in these images is under the age of 10. The images were embedded in the post such that they would have been downloaded to the user's computer and displayed on the user's computer screen upon accessing the post.

34. On February 28, 2015, the user "candygirl123" accessed the post entitled, "Kait aka Sugar" which was located in the "Pre-teen Videos", "Girls HC" section of "Website A". This post contained an embedded image, which I have viewed, is a compilation of 240 individual images that depicted what appeared to be prepubescent females engaged in oral and vaginal penetrative sexual activity with adult males. Some of the prepubescent females depicted appeared to be toddlers. The image was embedded in the post such that it would have been downloaded to the user's computer and displayed on the user's computer screen upon accessing the post. Additionally, after accessing the post, the user clicked directly on the described image which would have resulted in downloading another copy of the image to the user's computer.

35. Using publicly available websites, FBI Special Agents were able to determine that the above IP Address was operated by the Internet Service Provider ("ISP") Time Warner.

36. In March 2015, an administrative subpoena/summons was served to Time Warner Cable requesting information related to the user who was assigned to the above IP address. According to the information received from Time Warner Cable, the IP address was associated with David Tippens and a service address of 174 Jecelin St Unit #102, Wahiawa, HI 96786. Internet service was current as of March 23, 2015, at the aforementioned premises.

37. According to records obtained from the U.S. Army, David Tippens was stationed in Hawaii and resided at the above address from November 2014 until September 2015. These records show that as of March 2015, Tippens had three

dependents living with him, his two minor daughters (aged 14 and 16) and his mother, Mary Lynn Tippens.

38. In July 2015, the U.S. Army issued transfer orders for Tippens to relocate to Washington State, and he now resides at the SUBJECT PREMISES. Military records show that Tippens left Hawaii in September 2015.

39. On December 17, 2015, I spoke with officials from the University Place School District. They confirmed that Tippens's daughters are currently enrolled with the district and that the SUBJECT PREMISES is their address on file. They also reported that Mary Tippens moved out of the residence and away from Washington State sometime in November 2015. They were not sure of the exact date.

40. On January 13, 2016, I conducted surveillance of the SUBJECT PREMISES. I watched as Tippens left the home around 7:15 a.m. I also saw two vehicles: A four-door 2013 Ford Taurus sedan (Hawaiian License plate SBC313) and a 2014 Ford Explorer (Hawaiian License plate SCE184), both of which are registered to Tippens at his previous address in Hawaii.

41. Records checks using publicly available databases and records available from the Washington State Department of Licensing did not reveal any association between Tippens and the SUBJECT PREMISES. But this is likely explained by the fact of the family's recent relocation to Washington State from Hawaii.

42. On or about December 16, 2015, I received information from the United States Postal Service's ("USPS") Delivery Unit that services the SUBJECT PREMISES. USPS personnel indicated that mail was being delivered to the SUBJECT PREMISES that was addressed to David Wayne Tippens.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW [AND/OR COLLECT, RECEIVE, DISTRIBUTE OR ADVERTISE] CHILD PORNOGRAPHY

43. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement

officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view and possess, collect, receive, or distribute images of child pornography:

(a) Individuals who access with intent to view and possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

(b) Individuals who access with intent to view and possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

(c) Individuals who access with intent to view and possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

(d) Likewise, individuals who access with intent to view and possess, collect, receive, or distribute pornography often maintain their collections that are 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 or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

(e) Individuals who access with intent to view and possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

(f) Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

(g) Individuals who access with intent to view and possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

44. Based on the conduct set forth above, I believe that Tippens or a resident of the SUBJECT PREMISES likely displays characteristics common to individuals who access with the intent to view and/or, possess, collect, receive, or distribute child pornography.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

45. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers

basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

46. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

47. 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 (FTPs) to anyone with access to a computer and modem. 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.

48. 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 thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

49. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

50. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, 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 or external media in most cases.

51. 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. Such information is often maintained indefinitely until overwritten by other data.

SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

52. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

(a) Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

(b) Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. 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. Computer hard drives are now being sold for personal computers

capable of storing up to two terabytes (2,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

(c) Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

53. In this particular case, the government anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched, which will facilitate the search for evidence that does come within the items described in Attachment B. Further, the government anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and or suspected child pornography image files. Use of these tools will allow for the quick identification of evidentiary files but also assist in the filtering of normal system files that would have no bearing on the case.

54. Because multiple persons may share the SUBJECT PREMISES (to include the known occupants Tippens and his two juvenile daughters), it is possible that the SUBJECT PREMISES will contain computers or other digital media that are owned and exclusively used by persons who are not suspected of a crime. If agents conducting the search find multiple computers in the residence, they will attempt to corroborate, on site, which resident(s) has/have access to each computer. If agents have probable cause to believe that Tippens or one of his daughters has accessed or has used a particular

computer or digital device, agents will seize that particular computer or digital device and search it subject to the protocols set forth in this Affidavit.

55. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

(a) Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

(b) If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

(c) In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

(d) The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate

and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

(e) If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

56. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

(a) Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

(b) Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

(c) Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

(d) Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

(e) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

(f) Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

(g) Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

CONCLUSION

57. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the person of David W. Tippens futher described in Attachment A. I respectfully request that this Court issue a search warrant for these locations, authorizing the seizure and search of the items described in Attachment B.

Douglas Shook, Task Force Officer
Federal Bureau of Investigation

Sworn to me this 9th day of February, 2016.

KAREN L. STROMBOM
United States Magistrate Judge