JAP:MJJ

15M534

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS [redacted]
BROOKLYN, NY 11211

- X

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

(Fed. R. Crim. P. 41)

EASTERN DISTRICT OF NEW YORK, SS:

JOHN ROBERTSON, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS [redacted] BROOKLYN, NEW YORK 11211 (the "PREMISES"), the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of 18 U.S.C. § 2251(d) and (e) (advertising, attempting to advertise, and conspiracy to advertise child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography).

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I have been a Special Agent with the FBI since November 2006 and am currently assigned to the New York Office. Since February 2013, I have been assigned to a Crimes Against Children squad and have investigated violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through classroom training and daily work conducting these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous child pornography ("CP") cases and have reviewed thousands of photographs depicting minors being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of CP. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

---

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

I. DEFINITIONS

3. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct" and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ."[2]

c. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

d. The term "IP Address" or "Internet Protocol Address" means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

c. The term "Internet" refers to 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.

---

[2] *See also Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

d. The term "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

e. "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.

f. "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.

g. "Computer passwords, pass-phrases and data security devices," refer to 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, and reverse the progress to restore it.

II. BACKGROUND OF THE INVESTIGATION

A. "WEBSITE A"

4. A website ("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. 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.

5. 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 could not generally be accessed through the traditional Internet. 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.

6. 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.

7. Third party software ("Network Monitoring Program" or "Investigative Software") is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

8. 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 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.

9. 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.

10. 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. 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." 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."

11. 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.

12. 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.

13. 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 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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 states 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.

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

B. COURT AUTHORIZED USE OF NETWORK INVESTIGATIVE TECHNIQUE

19. 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.

20. 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.

21. 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.

22. Pursuant to that authorization, on or about and between February 20, 2015, and 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.

C. ACTIVITY OF "PLOWDEN 23" ON WEBSITE A

23. 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 "plowden23" engaged in the following activity on Website A.

24. The profile page of user "plowden23" indicated this user originally registered an account on Website A on September 3, 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 "plowden23's" profile, this user was a "newbie" Member of Website A. Further, according to the Statistics section of this user's profile, the user "plowden23" had been actively logged into the website for a total of 216 hours on or about and between September 3, 2014 and March 1, 2015.

25. According to data obtained from logs on Website A, monitoring by law enforcement, and the deployment of a NIT, on February 26, 2015, the user "plowden23" engaged in the following activity on Website A from IP address 67.243.156.191. During the session described below, this user browsed Website A after logging into Website A with a username and a password.

26. On February 26, 2015, the user "plowden23" with IP address 67.243.156.191 accessed the post entitled "Valya thread" in the section "Pre-teen Videos >> Girls HC". Based upon my training and experience I know that "HC" is a common acronym for "hardcore." Among other things, this post contained a set of 16 images that depicted a prepubescent female, wearing white stockings with a hole cut in the genital area. In two of the images the prepubescent female is depicted holding a phallic shaped object in or around her exposed genitals. Two of the images depict the prepubescent female bent over at the waist with the image focused on her exposed genitals and anus. Several of the remaining images depict the prepubescent female engaged in genital intercourse with an adult male.

27. During the following additional sessions, the user "plowden23" 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.

28. On February 25, 2015, the user "plowden23" accessed a post that contained a link to a series of 20 images that depicted a prepubescent female engaged in genital intercourse with an adult male. The final three images appear to depict the adult male ejaculating in or around the anus of the prepubescent female. A red mark that appears to be a rash is visible on the buttocks of the prepubescent female.

29. On February 26, 2015, the user "plowden23" accessed a post that contained a link to a set of 25 images that depicted an early pubescent female who appeared to be under the age of 18. In several images the camera is focused on the exposed genitals of the early pubescent female. In several images the early pubescent female is depicted inserting fingers into her vagina. In several images the early pubescent female is depicted performing oral sex on an adult male.

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

31. In or about February 2015, an administrative subpoena/summons was served to Time Warner Cable requesting information related to the user assigned to IP address 67.243.156.191. According to the information received from Time Warner Cable, an individual named [redacted] is the subscriber to whom IP address 67.243.156.191 is allocated. Time Warner Records also revealed that Martino receives internet service at the [redacted] Brooklyn, NY 11211, and has been receiving internet service there since approximately 2006. [redacted] Internet service was current as of April 27, 2015 at the aforementioned premises. The telephone number associated with Martino's account is [redacted]

32. A search of publicly available information on the Internet revealed that [redacted] is a website that features artwork produced by [redacted]. Posted to this website is a curriculum vitae that details the background of [redacted] residing at the PREMISES, and lists [redacted] as his telephone number.

33. This search also revealed a Facebook page belonging to an individual named [redacted] In or about July 2014, the user of this Facebook page posted the following message: [redacted]

34. A search of the Accurint database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) for the PREMISES revealed that [redacted] resides at the PREMISES.

II. THE PREMISES

35. On or about June 8, 2015, the undersigned affiant contacted ConEdison, a public utilities provider to the greater New York City area, regarding services provided to the PREMISES. A representative of ConEdison indicated that [redacted]s the financially liable party for the PREMISES, that the account is active, and that it has been active since approximately August 2005. The ConEdison representative also stated that utilities service is provided to the entire first floor of the PREMISES, and is not divided among subunits or rooms, in any, within Apartment 1.

36. The PREMISES comprise the ground floor of a three-story, brick and vinyl-sided row house on [redacted] in Brooklyn, New York. All residential tenants residing within the building, as well as PREMISES, appear to access the building through a main door on

the front of the building on the first floor, facing [redacted]. The entry door is off-white in color, and has the numbers [redacted] affixed to it.

37. Next to the entry door is a buzzer-entry system. There is only one buzzer for the first floor, and the number [redacted] appears next to it. There are separate buzzer buttons for apartments on floors [redacted]

III. CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

38. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

39. I know that some collectors of child pornography retain their materials and related information for many years. In my experience, collectors of CP who use the Internet to search for and collect CP often download video and image files that they find. By downloading CP and saving it to their personal computers or attached storage devices, collectors of CP can thereby view it at any time, without having to search for it later. Even in cases where collectors of CP attempt to delete or conceal their collection of CP, forensic examinations are often able to recover CP that remains within their computers or electronic storage devices. In this case, the user of the plowden23 account spent approximately 216 hours logged into Website A, which, as stated above, is not only difficult-to-find (as it requires knowledge of its very existence, use of special software to access it via the Network, and its specific address within that Network), but

more importantly, serves primarily to advertise and distribute CP. For this reason, I believe it is reasonable to infer that the user of the plowden23 account to have downloaded some of the CP posted to Website A during his 216 hours spent browsing therein.

40. I also know that some collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

41. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

42. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

43. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

IV. TECHNICAL BACKGROUND

44. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits or instrumentalities of violations of 18 U.S.C. § 2251(d) and (e), 18 U.S.C. § 2252A(a)(2)(A) and (b)(1), and 18 U.S.C. §

2252A(a)(5)(B) and (b)(2), that might be found on the PREMISES, in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

45. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on the evidence that a computer connected to a P2P network through an IP address registered at the PREMISES, there is reason to believe that there is a computer currently located on the PREMISES.

46. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic "attribution" evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online

nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.