4. The Proof Material must show different positions / poses of the Child ? all with the candle and sign visible.
5. The Proof Material must show must of the Childs Body. We do not accept close-ups images only.
6. The Proof Material can not be a part of the Entry Post. The proof is for the Admins only and the Entry Post for the other Producers.
We hope you understand that the strict requirements is for your own and the other Producers safety. No one likes the wrong people (scammers) to get into the Producers Boards.
We look forward to your application. The Admin Team.

23. No further Website A content was accessible to the undercover law enforcement officer, who did not apply for private or producer membership because of the website's requirement, described above, that users post specific child pornography in order to gain those levels of membership.

24. After registering an account via the "Registration" tab and logging into the site as a registered user, an additional tab entitled "My Messages" was observed in the same area as the "Home" tab. Further, a hyperlink was observed near the bottom of the home page entitled "Personal Messages" and the text "You've got 0 messages….Click here to view them." This "Personal Messages" function appeared to be a feature that allowed users to send each other private or "personal" messages.

THE NETWORK INVESTIGATIVE TECHNIQUE

25. Based on my training, experience, and the investigation described above, I have concluded that using a network investigative technique may help FBI agents locate the users of the child pornography Website A. Accordingly, I request authority to use the NIT, which will be deployed on Website A to investigate any user or administrator who logs into any of Website A by entering a username and password.

26. In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the website would augment that content with some additional computer instructions. When a computer successfully downloads those instructions from Website A, the instructions are designed to cause the "activating" computer to deliver certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of that computer.

27. The NIT will reveal to the government environmental variables and certain registry-type information that may assist in identifying the computer, its location, and the user of the computer, which constitute evidence of violations of the statutes cited in paragraph 5. In particular, the NIT will reveal to the government no information other than the following items, which are also described in Attachment B:

- The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
- A unique identifier (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier will be sent with and collected by the NIT;
- 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 has already been delivered to the "activating" computer;
- The "activating" computer's Host Name. A Host Name is a name that is 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;
- The "activating" computer's 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.

28. Each of these categories of information described in Attachment B may constitute evidence of the crimes under investigation, including information that may help to identify the "activating" computer and its user. The actual IP address of a computer that accesses Website A can be associated with an Internet service provider ("ISP") and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating

system running on the computer, the computer's Host Name, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

29. During the up to thirty day period that the NIT is deployed on Website A, each time that any user or administrator logs into Website A by entering a username and password, the NIT authorized by this warrant will attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government in [District].

REQUEST FOR DELAYED NOTICE

30. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(1) and (3) allows for any notice to be delayed if "the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) . . . ," or where the warrant "provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the users or administrators of Website A to undertake other measures to conceal their identity, or abandon the use of Website A completely, thereby defeating the purpose of the search.

31. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing Website A. It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn

the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).

32. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing Website A has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

33. The government further submits that, to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the NIT does not deny the users or administrators access to Website A or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

TIMING OF SEIZURE/REVIEW OF INFORMATION

34. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." The government requests authority to deploy the NIT onto Website A at any time of day, within fourteen days of the Court's authorization. The NIT will be used on Website A for not more than 30 days from the date of the issuance of the warrant.

35. For the reasons above and further, because users of Website A communicate on the board at various hours of the day, including outside the time period between 6:00 a.m. and 10:00 p.m., and because the timing of the user's communication on the board is solely determined by when the user chooses to access the board, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses Website A, even if that occurs outside the hours of 6:00 a.m. and 10:00 p.m. Further, I seek permission to review information transmitted to a computer controlled by or known to the government, as a result of the NIT, at whatever time of day or night the information is received.

36. The government does not currently know the exact configuration of the computers that may be used to access Website A. Variations in configuration, e.g., different operating systems, may require the government to send more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the activating computers for up to 30 days after this warrant is authorized.

37. The Government may, if necessary, seek further authorization from the Court to employ the NIT on Website A beyond the 30-day period authorized by this warrant.

SEARCH AUTHORIZATION REQUESTS

38. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. the NIT may cause an activating computer – wherever located – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location,

other information about the computer and the user of the computer, as described above and in Attachment B;

b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;

c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;

d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed Website A has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

CONCLUSION

39. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access Website A, in violation of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy

to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

40. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

41. Based on the information described above, there is probable cause to believe that employing a NIT on Website A, to collect information described in Attachment B, will result in the FBI obtaining the evidence and instrumentalities of the child exploitation crimes described above.

Sworn to under the pains and penalties of perjury.

_____
John Smith
Special Agent

Sworn to and subscribed before me
this _____ day of [ ], 20_____

_____
HONORABLE Jane Doe
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Locations to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography website referred to herein as Website A, as identified by the Tor URL example.onion, which is located in this district.

The activating computers are those of any user or administrator who logs into Website A by entering a username and password.

The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. 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);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's media access control ("MAC") address;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.