Understanding a Search Warrant for Digital Evidence Assignment Instructions

This assignment is in two parts. The first section will ask you to answer questions about search warrants. You can answer these questions by listening to the audio recording. The second section will ask you to select and analyze a warrant for digital evidence. You can download this document and answer your questions directly on the form.

Part 1

1. According to the audio (or Fitzsimmons' article), what are the three requirements for writing a good search warrant for digital evidence? (10 pts)
   Understanding the technology involved in the case, understanding the requirements of the Fourth Amendment's "Warrants Clause," and establishing a nexus between the evidence you hope to find and the underlying crime.
2. What is meant by "establishing a nexus between the evidence and the crime?" (15 pts)
   The nexus provides logical explanations between probable cause to search or seize, which enables a judge to understand the connection and grant a search warrant. It also provides additional support against a defense challenging the search warrant.
3. What does "affiant" mean? (5 pts)
   An affiant is a person who swears to an affidavit.

4. Which type of law enforcement officer must complete an affidavit for a search warrant? _____ (5 pts)
    a. Local police (e.g., Norfolk PD)
    b. State police (e.g., Virginia State Police)
    c. Federal agencies (e.g., Federal Bureau of Investigations)
    d. All of the above

Part 2

Select a file from the folder corresponding to the first letter of your last name (A - H, I - P, or Q - Z). Each folder contains several affidavits for a search warrant. After choosing one to your liking, answer the questions below. Affidavits for warrants will vary in length, so summarize whenever possible. Also, some information may be redacted, and you will need to work around these redactions. You can still answer all the questions.

5. What is the name of your search warrant (filename on Google Doc)? (5 pts.)
   Plowden
6. What is the name of the officer requesting a search warrant? (5 pts.)
   John Robertson
7. What expertise does the officer have? (5 pts.)
   He is a special agent with the FBI and has been since 2006. He was assigned to a Crimes Against Children squad in 2013.
8. Where is the search taking place? (5 pts.)
   Brooklyn, New York
9. What cybercrime is the person to be searched accused of? The crime will be written in legalese so use laymen's terms when possible. Remember from CRJS 310, unauthorized access is "hacking," nonconsensual sharing of images is "revenge porn," and so on. (5 pts)

The cybercrime the person is being accused of is the use, distribution, and reproduction of CP.

10. What evidence is the officer looking for? (if it is several pieces, just select a few) (5 pts.) The officers are looking for the multimedia storage devices (hard drives, thumb drives, solid state drives) in which the CP was stored or shared from the suspect's residence.
11. In a few sentences, describe how the officer establishes probable cause? (15 pts.) He takes a look at all the evidence that has been gathered; IP information, reconnaissance from Website A where this media has been shared and posted, and the user information that has been shared by the ISP for this particular individual. This information is referred to and used to draft a warrant.
12. In a few sentences, explain how the officer establishes a nexus between the evidence and the crime (10 pts.) The officer uses the digital records, such as IP information and files pertaining to the crime. He also uses the written descriptions of the categories of CP listed and posted on the site as a connection between the evidence and the crime committed.
13. Do you think an officer needs special training in order to investigate cybercrimes? Why or why not? (10 pts) Officers do require specific training in order to investigate cybercrimes. Cybercriminals employ dynamic tactics and intricate digital technologies to commit cybercrimes. Officers who receive specialized training are better able to navigate digital environments, comprehend pertinent laws and regulations, gather digital evidence, and work with experts in digital forensics. Officers might find it difficult to recognize, look into, and prosecute cybercrimes without this training, which would leave offenders unchecked and victims unprotected. Thus, in order to guarantee that law enforcement organizations can successfully counter

cyberthreats and protect communities in the digital age, specialized training is crucial.