AFFIDAVIT OF ROBERT ERDELY

1. This affidavit is regarding the motion titled "C-4 Motion to Compel Discovery and Production of Evidence" in *United States v. Matthew Schwier*, 3:17-cr-0095-SLG.

2. My credentials were previously set forth in my Affidavit filed at Dkt 214-1 and 214-2. Additionally, definitions and descriptions of the BitTorrent P2P Network and the ICAC Law Enforcement System were previously set forth in my Affidavit filed at Dkt. 214-1. I incorporate my credentials, definitions and background information as if fully set forth herein.

3. This affidavit is a supplementation of my previously prepared affidavit filed at Dkt. 214-1. In this affidavit I will address the declaration filed by Mr. Fischbach at Dkt. 203-1.

Analysis of Defense Expert's affidavit

4. I discussed this investigation with AUSA Jonas Walker who provided the defense experts declaration in this case. The following are my responses related to details found in Jeffrey M. Fischbach's declaration.

5. In paragraph 3, Mr. Fischbach states: "The authenticity of the file allegedly downloaded by the FBI on or about November 22, 2016 remains in question. There has been no evidence produced, thus far, that the file used to substantiate the search of Mr. Schwier's property was ever on any media or device associated with Mr. Schwier. Based on my review of the discovery provided by the government this file was not found on any digital media seized from Mr. Schwier's residence. At this time, there is no known modified, accessed or creation (MAC) dates or times for this file. Similarly, there has been no metadata, typically used for the purposes of authenticating a file, its origin, dominions, and chain of custody. Most concerning to me, is that I have been unable to elicit from the government any of this forensically-crucial material, specific to the file the FBI claims to have downloaded remotely from Mr. Schwier -- the file which justified a search warrant, and subsequent arrest."

RESPONSE: During the investigation, through the use of Torrential Downpour (TD), the downloaded material is saved to a directory named "download". The associated log files are contained in the "logs" directory. The logs associated with this investigation detail the date and time when the investigation begins along with other details. Regarding Mr. Fischbach's request, the dates and times when the file was downloaded is found in the "details.txt" file which is contained within the logs directory. It is my

understanding that this information has already been provided in discovery. This log will provide information as to the date and time the file began the downloading process, the dates and times which each piece of data was received during this investigation and the date and time the download had completed the downloading process. The MD5 and SHA1 hash value of the entire file is located at the bottom of this log file. It also provides information regarding the SHA1 hash verification of every piece downloaded from the suspect computer, where the data downloaded is compared to the values contained within the .torrent file (the instructions). Through the downloading of the file, and this checking of each and every hash value of the pieces received, only a computer possessing the file could have distributed the data to the investigative computer.

6. In paragraph 4, Mr. Fischbach states (in part): "The data provided in response to my request is a Bit Torrent log file, which does not provide any information sufficient to extrapolate chain of custody or determine authenticity."

RESPONSE: Mr. Fischbach's claim that the log file does not provide any information to determine the downloaded files authenticity is incorrect. As stated above it contains not only the hash value of the file but each and every piece hash and the verification of those pieces using the SHA1 hashing algorithm.

7. In paragraph 6, Mr. Fischbach states (in part): "A copy of the file stored on some other media provides little to no authentication information about how or when the file was "captured." The original media itself contains that information."

RESPONSE: Mr. Fischbach's claim above is incorrect. Given the fact that accompanying the file downloaded is the detailed log, the SHA1 hashing of the pieces along with the verification of those pieces should provide any expert the means necessary to verify that this is the file associated with the .torrent being investigated. Using the same hashing method used by the BitTorrent file sharing network, the expert can independently verify that this is the file relating to the download conducted. I will make available all of the files associated with the .torrent being investigated and a SHA1 hashing report of those files, confirming that these are in fact all the files described by the .torrent to aid him in his analysis. As the lead instructor of this investigative software and a user of the software (TD), giving a defense expert access to the investigative computer would provide him with access to the investigative software itself and potentially expose him to details of active investigations.

8. In paragraph 9, Mr. Fischbach states (in part): "It is imperative for me to inspect and examine all metadata, as well as determine the file's true and accurate file

name, file size, and file path, the means by which it was captured and preserved, determine a valid hash value".

RESPONSE: Mr. Fischbach has received the details.txt (the detailed logging of the investigation) which includes details regarding the file, including not only the files SHA1 hash value of any completed download, but also the hash value of every piece of data downloaded. Examining the .torrent file being investigated include the following:

- file names
- file paths
- file sizes
- piece size
- SHA1 piece hashes

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge and belief.

Detective Robert W Erdely
Date: 9-19-2019