Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	Case No. 3:17-cr-0095 SLG
	)	
vs.	)	
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	
	)	

C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE

A period of excludable delay under 18 U.S.C.§3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. A total of 36 days remain before trial must commence pursuant to the Speedy Trial Act.

Comes now, Defendant, Matthew Schwier, by and through counsel, Robert M. Herz, of the Law Offices of Robert Herz, P.C. and hereby moves this court, pursuant to the fifth and sixth amendment of the United States Constitution, and as well Federal Rule of Criminal Procedure 16, and *Brady v.* Maryland, 373 U.S. 83 (1963) and its progeny, for an order compelling the government to provide discovery and produce evidence of a copy of the Torrential Downpour software used by the government in its undercover investigation in this case between October 20 and November 24, 2016, those dates being approximate.

BACKGROUND FACTS

A. The Indictment.

On April 26, 2019 the government filed a third superseding indictment in this case. Mr. Schwier was arraigned on the new indictment on May 1, 2019. Count 1 of the third superseding indictment reads as follows:

> On or about October 20, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, did ***knowingly possess, and knowingly access*** with intent to view, any computer disk, and any other material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8)(a), that has been mailed, and shipped and transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that have been mailed, and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Any image of child pornography involved in the offense involved a prepubescent minor and a minor who had not attained 12 years of age. All of which is in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2).

Emphasis supplied.

Count 2 of the third superseding indictment reads as follows:

> On or about November 22, 2016, to November 24, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, did **knowingly distribute** any child pornography, as defined in 18 U.S.C. § 2256(8)(a), that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. All of which is in violation of 18 U.S.C. § 2252A(a)(2)(A), (b)(1).

Emphasis supplied. Of note, in this iteration of the distribution count, the government simply claims that Mr. Schwier did "knowingly distribute *any* child pornography...." The government does not specify an image or provide a file designation nor describe the number of images distributed. However, the government will concede only one act of "distribution" allegedly transpired in this case when the FBI allegedly downloaded and

received one file alleged to contain child porn. A comparison of this iteration of the charge to how it was written in the Second Superseding Indictment is illustrative. Count 2 in the Second Superseding indictment reads as follows:

> On or about November 22, 2016, to November 24, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, ***did knowingly distribute***, by any means and facility of interstate and foreign commerce, a visual depiction of a minor engaging in sexually explicit conduct, ***to wit: "1180842565051.jpg,"*** the production of which involved the use of minors engaging in sexually explicit conduct. The production of the visual depiction involved a prepubescent minor and minor under 12 years of age engaging in sexually explicit conduct and the visual depiction was of such conduct. All of which is in violation of 18 U.S.C. § 2252(a)(2), (b)(1).

Emphasis supplied.

As the court can see, in the Second Superseding Indictment the government specifies a single and sole image as allegedly distributed, and indeed, that is the only file the FBI claims that it ever downloaded and received, based on all the discovery provided by the government to date.

B. The Investigation

1. The October surreptitious searches.

According to SA Allison's affidavit in support of the search warrant application, 3:17-mj-00198 DMS, dated April 28, 2017, on or about October 20, 2016 he conducted a surreptitious search of an IP address, later identified as being associated with Mr. Schwier. The agent attempted to download data from the identified IP address, using an FBI modified program of the bitTorrent protocol. This FBI modified program is only available to law enforcement and is known as "Torrential Downpour." This FBI program has never been scientifically validated or verified to be reliable by any

independent third party and shown to work in the manner claimed by the FBI. The FBI program attempted to download data, identified by a specific hash value, believed to contain child pornography. According to the agent, the hash value represents 3439 pieces of data representing a total of 66 files. Allegedly the target IP address "acknowledged" that it had 1387 pieces of data *none of which were downloaded or received by the FBI*. In addition, the modified FBI program allegedly reported that the IP address "possessed" 45 of the files. According to the SA Allison 6 of these files contain child porn based on a review of archived FBI files. *None of those files were downloaded or received by the FBI.*

Later that same day, the FBI program made a second attempt to download data from the same target IP address. The attempt to download data again used an indentified hash value believed to contain child porn. This hash value, according to the agent, contains 6595 pieces of data and represents 249 files. Of these, the FBI program allegedly identified the IP address as having 6474 pieces of the data and 204 complete files. Based on a review conducted by SA Allison of FBI archived files, allegedly 74 of these files contain child porn. However, as before during the first attempt, *none of the 6474 pieces of data were downloaded or received by the FBI, and none of the files were downloaded or received by the FBI.* See, paragraphs 22-23 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS.

2. The November surreptitious searches. The FBI again experienced problems downloading files just as it had during the October 2016 surreptitious searches.

According to SA Allison's affidavit in support of the search warrant application, 3:17-mj-00198 DMS, dated April 28, 2017, on or about November 20, 2016 between 7:23 p.m. and 7:27 a.m. the next day, he conducted a surreptitious search of an IP address, later identified as being associated with Mr. Schwier. The agent attempted to

download data from the identified IP address, using an FBI modified program of the bitTorrent protocol. The FBI program attempted to download data, identified by specific hash values, believed to contain child pornography. According to the agent, the hash values represent 1545 pieces of data representing a total of 306 files. Allegedly the target IP address "acknowledged" that it had all 1545 pieces of data *none of which were downloaded or received by the FBI*. In addition, the modified FBI program allegedly reported that the IP address "possessed" all 306 of the files. According to SA Allison 28 of these files contain child porn based on his review of archived FBI files. *None of those files were downloaded or received by the FBI.*

On that same day, the FBI program made a second attempt to download data from the same target IP address between 7:43 p.m. and 8:26 p.m.. The attempt to download data again used an indentified hash value believed to contain child porn. This hash value, according to the agent, contains 543 pieces of data and represented one (1) file. The FBI program allegedly identified the IP address as having all 543 pieces of the data and the one (1) complete file. Based on SA Allison's review of FBI archived files, allegedly the one file contained child porn. However, as before, during the first attempt, *none of the 543 pieces of data were downloaded or received by the FBI, and none of the single file was downloaded or received by the FBI.* See, paragraphs 24-25 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS.

On November 22, 2016 a third search of the identified IP address was initiated. This third attempt to download data began on November 22 at 8:48 p.m. and ended on November 24, 2016 at 9:02 p.m. The attempt to download data again used an identified hash value believed to contain child porn. This hash value, according to the agent, contains 4861 pieces of data and represents 5616 files. Of these, the FBI program allegedly identified the IP address as having 4619 pieces of the data and 5309 complete

files. This time two files were completely downloaded and received by the FBI. No other pieces of data and no other files alleged to be "possessed" were downloaded or received by the FBI. Based on SA Allison's review of the two files received, only one file was determined by the agent to contain child porn. The file designation for that file is 1180842565051.jpg. See, paragraphs 26 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS. It is this one file that forms the basis of count 2 in the Third Superseding Indictment.

C. The Forensic Search Of Mr. Schwier's Hard Drives.

1. The subsequent FBI search found nothing related to any putative data or files from October 20, 2016 on any of Mr. Schwier's computers or hard drives.

The search warrant application was granted by the court on April 28, 2017 and a search of Mr. Schwier's residence commenced on May 1, 2017. A number of electronic media were seized, including several computers containing internal hard drives, and some external hard drives as well. Subsequent to these items being seized they were forensically analyzed by Agent Allison. Agent Allison reported the results of this forensic evaluation in two "FBI 302s" dated respectively July 7 and July 12, 2017. None of the data or files, and no fragments of any of these files, allegedly identified as being "acknowledged" or "possessed" on October 20, 2016 were found on any media seized from Mr. Schwier. Moreover, AUSA Walker indicated during a hearing before this court on March 25, 2019, that for purposes of count 1 in the Second Superseding Indictment (which alleges the same conduct as in Third Superseding Indictment) that the government could not specify or identify the particular "matter' or hard drive seized from Mr. Schwier on which any contraband alleged to be possessed on or about October 20 was alleged to be found for purposes of count 1 of the indictment.

2. The subsequent FBI search of hard drives and computers seized from Mr. Schwier's residence found nothing related to any putative data or files from November 20, 2016 through November 24, 2016 on any of Mr. Schwier's computers or hard drives, including the one file allegedly "distributed."

None of the data or files, and no fragments of any of these files, allegedly identified as being "acknowledged" or "possessed" on or about November 20 to November 24, 2016 were found on any media seized from Mr. Schwier. There was no trace of the file allegedly downloaded and comprising the file designation 1180842565051.jpg that is the basis for count 2. Defense requests to have access to and to inspect and examine the original file on the original media upon which it was saved by the government when it was downloaded and that comprises 1180842565051.jpg have been denied by the government. The defense requires access to the original file to attempt to determine its actual origins and to authenticate it.

D. The BitTorrent Network and Torrential Downpour.

The indictment in this cases alleges that Mr. Schwier downloaded and shared child pornography files using the BitTorrent file-sharing network. BitTorrent is an online peer-to-peer network that allows users to download files containing large amounts of data, such as movies, videos, and music. Instead of relying on a single server to provide an entire file directly to another computer, which can cause slow download speeds, BitTorrent users can download portions of the file from numerous other BitTorrent users simultaneously, resulting in faster download speeds.

To download and share files over the BitTorrent network, a user must install a BitTorrent software "client" on his computer and download a "torrent" from a torrent-search website. A torrent is a text-file containing instructions on how to find, download, and assemble the pieces of the image or video files the user wishes to view. The client software reads the instructions in the torrent, finds the pieces of the target file from

other BitTorrent users who have the same torrent, and downloads and assembles the pieces, producing a complete file. The client software also makes the file accessible to the other BitTorrent users in a shared folder on the user's computer.

Torrential Downpour is law enforcement's modified version of the BitTorrent protocol. Torrential Downpour acts as a BitTorrent user and searches the internet for internet protocol ("IP") addresses offering torrents containing known child pornography files. When such an IP address is found, the program connects to that address and attempts to download the child pornography. The program generates detailed logs of the activity and communications between the program and the IP address. Unlike traditional BitTorrent programs, the government claims that Torrential Downpour downloads files only from a single IP address – rather than downloading pieces of files from multiple addresses – and does not share those files with other BitTorrent users.

E. The Investigations into Defendant's BitTorrent Activity.

As previously noted in October 2016, Agent Allison used Torrential Downpour to identify an IP address which allegedly was making known child pornography files available on the BitTorrent network. Agent Allison allegedly used Torrential Downpour to connect with this IP address to attempt to download child pornography files on several occasions between October 20, 2016 and November 24, 2016. Presumably had he successfully downloaded any files he would have reviewed the Torrential Downpour activity logs to confirm that the program downloaded complete files solely from this IP address, and would have reviewed the files to confirm that they were child pornography.

Through further investigation, Agent Allison learned the subscriber information for the IP address. He obtained a search warrant for the subscriber's residence, and FBI agents searched the residence on May 1, 2017. They found several items of computer

equipment including several hard drives; all of the equipment was then seized. Mr. Schwier has never made any admission that he had used any computer to knowingly find, download, view or distribute any child pornography. As noted before forensic examinations of the seized media failed to find any of the files allegedly possessed on October 20, or on November 20, or on November 22-24. The forensic examination performed by the FBI did reveal child pornography images on four of the hard drives seized; many of the images though were duplicative of each other. Almost all of the images were thumbnails in a thumbnail cache which could not viewed, manipulated, or distributed by anyone unless using a forensic toolkit available to law enforcement. Notably the file that Torrential Downpour allegedly had downloaded from the IP address was not found on any hard drive or any other seized device.

The government has charged Mr. Schwier with one count of distributing child pornography and three counts of possessing such material. The distribution count is based on the file that Torrential Downpour allegedly downloaded on or about November 22, 2016. The possession counts are based on the child pornography found on the hard drives after the search.

ARGUMENT

Mr. Schwier contends that the Torrential Downpour software is flawed and should be tested and verified by a third party. He also contends that he needs access to the program in order to prepare effective cross examination of Agent Allison and the potential presentation by his own computer expert. Mr. Schwier seeks disclosure of an installable copy of the software pursuant to Federal Rule of Criminal Procedure 16, *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). He also seeks disclosure of Torrential Downpour's user and training manuals. He does not seek the program's source code.

Under Rule 16(a)(1)(E), the government must disclose any "books, papers, documents, data, . . . or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense[.]" To obtain disclosure under subsection (i), "[a] defendant must make a 'threshold showing of materiality[.]'" *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present *facts* which would tend to show that the [g]overnment is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added); *see also Budziak*, 697 F.3d at 1111-12.

A. Brady v. Maryland

Brady v. Maryland, 373 U.S. 83 (1963), requires the government to disclose to a defendant any and all evidence favorable to him if the evidence is material to guilt or to punishment. The good or bad faith of the prosecution in withholding the evidence is irrelevant: it must be disclosed, even if doubtful, and failure to recognize the evidence does not save the prosecutor from a violation. *Id.* At 87; *Strickler v. Greene*, 527 U.S. 263 (1999); *Youngblood v. West Virginia*, 547 U.S 867 (2007). Under *Brady* and its progeny the "prosecution," which includes the prosecuting attorney as well as the investigating agencies, must disclose favorable information that is, or is known to be, in its possession. *Strickler* at 263; *Kyles v. Whitley*, 514 U.S. 419 (1995); *Jackson v. Brown*, 513 F.3d 1057 (9th Cir. 2008).

The duty of disclosure extends to evidence relating to the credibility of witnesses. *Strickler* at 263, *Giglio v. United States*, 405 U.S. 150, 154 (1972). The existence or nonexistence of a defense request for the evidence is immaterial to the

prosecution's duty to produce it. *Strickler* at 263; *United States v. Agurs*, 427 U.S. 97, 107 (1976). Even evidence the prosecutor regards as inherently improbable must be disclosed. *In re Chol Soo Lee*, 103 Cal.App.3d 615, 618-619 (1980). "Impeachment evidence … as well as exculpatory evidence, falls within the Brady rule." *United States v. Bagley*, 473 U.S. 667, 676 (1985). "When the 'reliability of a given witness may well be determinative of guilt or innocence' nondisclosure of evidence affecting credibility falls within this general rule." *Giglio v. United States*, 405 U.S. 150, 15355 (1972). Thus, the prosecution violates due process by "fail[ing] to disclose evidence that the defense might" use "to impeach the Government's witnesses by showing bias or interest." *Bagley*, 473 U.S. at 676. The information need not be admissible so long as it "is likely to lead to favorable evidence that would be admissible." *United States v. Sudikoff,* 36 F.Supp.2d 1196, 1200 (C.D. Cal 1999).

"The prosecution's duty to reveal favorable, material information extends to information that is not in the possession of the individual prosecutor trying the case." *Amado v. Gonzalez*, 758 F.3d 1119, 1134 (9th Cir. 2014). In particular, it extends to police officer witnesses. *See e.g., United States v. Price*, 566 F.3d 900, 903 (9th Cir. 2009) (reversing and remanding where federal prosecutors failed to learn of exculpatory evidence in the state police's control). The prosecution's duty also extends to situations where there is a dispute between the parties about the significance of the information. The prosecution should not "confuse[] the weight" to be given *Brady* evidence "with its favorable tendency." *Kyles*, 514 U.S. at 451. In order to qualify, the evidence need only have "some weight" that is "favorable" to the defense. *Id.* "[T]he Suprement Court has pronounced that if a prosecutor has doubt about certain evidence' exculpatory value, the prosecutor should err on the side of disclosure." *Schledwitz v. United States*, 169 F.3d 1003, 1014 n.4 (6th Cir. 1999)(citing Kyles); *United States v. Agurs*, 427 U.S. 97, 108

(1976); *see also United States v. Van Brandy*, 726 F.2d 548, 552 (9th Cir. 1984) ("[t]he government, where doubt exists as to the usefulness of evidence, should resolve such doubts in favor of full disclosure").

B. United State's Attorney Manual

In addition, the United States Attorney's Manual rigorously encourages prosecutors "to seek all exculpatory and impeachment information from all members of the prosecution team. Members of the prosecution team include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. U.S. Dept. of Justice, Justice Manual, § 9-5.001, "Policy Regarding Disclosure of Exculpatory and Impeachment Information." This policy guides federal prosecutors to probe carefully and to "disclose information that is inconsistent with any element of any crime charged against the defendant or that establishes a recognized affirmative defense, regardless of whether the prosecutor believes such information will make the difference between conviction and acquittal of the defendant for a charged crime." *Id.* at 9.5001.C. The manual provides for broad interpretation of "impeachment information": "A prosecutor must disclose information that either casts a substantial doubt upon the accuracy of any evidence—including but not limited to witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information must be disclosed regardless of whether it is likely to make a difference between conviction and acquittal of the defendant for a charged crime" *Id.*

C. Discoverability of Investigative Software.

The Ninth Circuit has addressed the discoverability of government software programs used to investigate child pornography offenses.

Mr. Schwier relies primarily on *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), and cases that have adopted its reasoning. *Budziak* involved the FBI's use of an enhanced version of the LimeWire file-sharing program called "EP2P." *Id.* at 1107. Using that program, the FBI downloaded several child pornography files from an IP address registered to Budziak. *Id.* A forensic examination of his computer revealed multiple child pornography files, including several images the EP2P program had downloaded. *Id.* Budziak was charged with multiple counts of distributing and possessing child pornography. *Id.* The district court denied Budziak's motions to compel disclosure of the government's EP2P program, and he was convicted on each count. *Id.* at 1107-08.

On appeal, the Ninth Circuit held that the district court abused its discretion in denying Budziak's motions to compel. It noted that he did more than assert a generalized need to review the EP2P program before trial; he identified particular defenses to the distribution charges that discovery on the EP2P program could help him develop. *Id.* at 1112. Specifically, he "presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his 'incomplete' folder, making it 'more likely' that he did not knowingly distribute any complete child pornography files to [the FBI]." *Id.* at 1112. He also presented "evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings." *Id.* Given this evidence, the Ninth Circuit concluded that "access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Id.*

Other cases have followed *Budziak*. For example, the district court in *United States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at *7 (D.N.M. Apr. 3,

2013), required the government to allow the defense expert to examine and use a copy of the government's confidential Shareaza software at a secure government facility. The court did so because the defendant in *Crowe*, like the defendant in *Budziak*, presented specific evidence to suggest that access to the software was material to preparing the defense. *See id.* Specifically, the defense expert testified that "some of the files alleged to have been found by law enforcement in the shared space of Defendant's computer, were not found there during her analysis." *Id.* See also, *U.S. v. Gonzales*, 2:17-cr-01311-DGC (D.AZ)(Order of court at Doc. 51, filed Feb.19, 2019, ordering disclosure of Torrential Downpour software); *U.S. v. Hartman*, 8:15-cr-00063-JLS (Cen.D. Cal)(Order of court at Doc. 87, filed Nov.24, 2015, ordering disclosure of government proprietary software Peer Spectre and ShareazaLE).

In *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015), the court of appeals affirmed a district court decision denying discovery of the "law enforcement tools" used to locate and download child pornography from the defendant's computer. The Sixth Circuit distinguished *Budziak,* noting that Budziak had presented the evidence just described *supra*. 787 F.3d at 365-67. The defendant in *Pirosko*, by contrast, "failed to produce any such evidence, simply alleging that he might have found such evidence had he been given access to the government's programs." *Id.* at 365. As a result, discovery was not warranted. *Id.*[1]

---

[1] *See also United States v. Jean*, 891 F.3d 712, 715 (8th Cir. 2018) (affirming denial of motion to compel government software because the defendant was convicted of receiving and possessing child pornography and "the likelihood of any help to [his] defense was 'vanishingly small'"); *United States v. Chiaradio*, 684 F.3d 265, 277 (1st Cir. 2012) (expressing no view on whether the EP2P source code was discoverable under Rule 16 where the defendant "neither contradicted nor cast the slightest doubt upon" the government's evidence that the FBI had downloaded child pornography from his computer); *United States v. Blouin*, 2017 WL 2573993, at *3 (W.D. Wash. June 14, 2017) (denying motion to compel

Budziak is, of course, binding precedent for this Court. The distinction between it and the *Pirosko* line of cases, just noted, is consistent with traditional Rule 16 principles. As already noted, "[n]either a general description of the information sought nor conclusory allegations of materiality suffice [under Rule 16(a)(1)(E)(i)]; a defendant must present *facts* which would tend to show that the [g]overnment is in possession of information helpful to the defense." *Mandel*, 914 F.2d at 1219 (emphasis added). In *Budziak* and *Crowe*, the defendants presented evidence to support their contention that discovery of the government software was material to preparing their defense to distribution of child pornography. In the other line of cases, they did not.

D. Mr. Schwier Has Shown Materiality.

Counts one and three allege violations of 18 U.S.C. § 2252A(a)(5)(B) and count two alleges a violation of 18 U.S.C. § 2252A(a)(2)(A). The latter section provides criminal punishment for any person who "knowingly receives or distributes, any child pornography ….. using any means or facility of interstate or foreign commerce . . . including by computer, . . ." Evidence is sufficient to support a conviction for distribution under § 2252A(a)(2) "when it shows that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it." *Budziak*, 697 F.3d at 1109.

---

where the defendant did not dispute that the government's software downloads files from a single source); *United States v. Maurek*, No. CR-15-129-D, 2015 WL 12915605 at *3 (W.D. Okla. Aug. 31, 2015) (denying motion to compel where the defendant failed to present specific facts which would tend to show how disclosure of Torrential Downpour would be material to his defense);

Mr. Schwier disputes and certainly casts doubt on whether the government downloaded any child pornography from any device possessed by him, and he disputes that Torrential Downpour consistently works as intended and is free from "bugs" so that it always and reliably downloads from a single source. Mr. Schwier maintains that Torrential Downpour is material to his defense because the distribution charge, Count 2, is based on a child pornography file that Torrential Downpour purportedly downloaded from his computer hard drive but that was not found on any hard drive or other device associated with Mr. Schwier when it was seized by the FBI. Torrential Downpour is also material to his defense because Count 1 specifically alleges he knowingly possessed child pornography on October 20 based on the surreptitious search conducted using Torrential Downpour. The government claims that the Torrential Downpour software allegedly identified and confirmed that child porn files were on a device using a specific IP address later found to be associated with Mr. Schwier. Yet none of those files or even fragments of those files were ever found on any device seized from Mr. Schwier's residence.

Mr. Schwier has presented an affidavit from his expert, Jeffrey M. Fischbach, confirming that the files are not on any device. Fischbach explains in his Declaration that it is critical to Mr. Schwier's defense to understand how Torrential Downpour functions in order to determine the program's reliability and accuracy in identifying the file that Mr. Schwier is charged with knowingly distributing or possessing. *Id.* at ¶ 29. He further states that based on his many years of research and testing of peer-to-peer file sharing software, including BitTorrent, he has discovered that all of these programs "contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable." *Id.* ¶ 22. Fischbach has opined that all software programs have flaws, and Torrential Downpour is no exception. He bases this opinion on his work in other cases involving Torrential

Downpour and the fact that the files the program allegedly downloaded in this case were not found on Schwier's devices. *Id.* at ¶ 21. Fischbach also provided a plausible explanation for how Torrential Downpour may have erroneously identified Schwier's computer as offering child pornography files over the BitTorrent network. Fischbach explained that, because a torrent is simply a text-file containing the hash values – or "fingerprints" – of the target image and video files, a BitTorrent user who downloads a torrent has fingerprints of the target files, even if he has not yet downloaded them. *Id.* at ¶ 15. Fischbach stated that the actual downloading of the target files occurs only when the client software instructs the torrent to search for those files on the BitTorrent network and download them to a designated folder on the user's computer. *Id.* at ¶ 14. He further stated that a forensic examination of the device used to download the torrent can determine whether the torrent has been used to download the file, and his examination of Schwier's devices revealed no evidence suggesting that he downloaded any files listed that might pertain to counts one through three. Id at ¶ 18. Fischbach opined that Torrential Downpour may have obtained the files from other BitTorrent users, particularly in light of the fact that this is how peer-to-peer file sharing programs are designed to work. *Id.* at ¶ 17.

This evidence brings this case squarely within the holding of *Budziak*. Mr. Schwier has done more than simply request access to the software and argue that it is material to his defense. He has presented evidence that calls into question the government's version of events. Given his evidence, this Court must find that "the functions of the [program] constitute[] a 'very important issue' for [Schwier's] defense." *Budziak*, 697 F.3d at 1112 (quoting *United States v. Cedano-Arellano*, 332 F.3d 568, 571 (9th Cir. 2003)); *see Crowe*, 2013 WL 12335320, at *7.

Where a defendant has demonstrated materiality, the Court "should not merely defer to government assertions that discovery would be fruitless." *Budziak*, 697 F.3d at

1112-13. Mr. Schwier "should not have to rely solely on the government's word that further discovery is unnecessary." *Id.* at 1113. Because Mr. Schwier has shown that the Torrential Downpour is material to his defense, he should be given access to the program to investigate its reliability and help him prepare for cross-examination of Agent Allison.[2]

Mr. Schwier also contends that Torrential Downpour is material because the program "searches beyond the public domain, essentially hacking computers as it searches for suspect hash values, and over-rides the computer's settings that otherwise would make files unavailable to be shared.

Mr. Schwier is charged with distributing child pornography based on the government's claim that the FBI, after apparently at some point identifying his computer as a download candidate for child pornography, infiltrated his computer on October 20, 2016 and attempted to download files. According to the Torrential Downpour software there were allegedly numerous suspect files on the computer. Yet, none of these attempts were successful. The FBI infiltrated his computer again in late November, again according to the software there were numberous suspect files on the computer. Again the FBI attempted to download files, and again all these attempts were unsuccessful, except for two suspect files that were successfully downloaded, and only one that was "verified" to be a prohibited image. Later when the computer hard drive was forensically searched, none of the identified suspected files that

---

[2] Even if the government were to present a log file purportedly showing that Agent Allison used Torrential Downpour to download from Schwier's device the child pornography file listed in count 2 of the Second Superseding Indictment, and that presumably forms the basis for count 2 in the Third Superseding Indictment, this log file cannot independently confirm that Agent Allison downloaded a complete child pornography file solely from Schwier's device. Since the log files were created by Torrential Downpour, if the program is flawed in the ways Schwier suggests, these log files would be flawed as well.

Torrential Downpour identified as being on the computer were found on the hard drive. Moreover, the one image that was "successfully" downloaded and "verified" to be a prohibited image also was not found on any hard drive possessed by Mr. Schwier.

The FBI could not find any of the files described by Torrential Downpour as being present and as described in the search warrant affidavit on any of the devices seized from Mr. Schwier. Apart from the allegation of "distribution" in the warrant affidavit, there is no evidence that Mr. Schwier ever physically distributed child pornography to another person. Mr. Schwier may defend the distribution allegation on the basis that he did not knowingly allow others to access files on his computer, and that Torrential Downpour overrode his computer's settings which were set so as to not share files on the BitTorrent software client. This defense requires access to the Torrential Downpour program. In identical circumstances, the Ninth Circuit ruled that defendant is entitled to discovery of special law enforcement software used to investigate him. *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012). The court found disclosure of the government software was material to the defense to show that law enforcement may have downloaded only fragments of files from his "incomplete folder; to show that "agents could have used the EP2P software to override his sharing settings"; and because "access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Id* at 1112. The Court held that "the functions of the EP2P software constituted a 'very important issue' for Budziak's defense. Given that the distribution charge against Budziak was premised on the FBI's use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense." *Id.*

Here, the sole evidence of distribution arises from Agent Allison's use of the Torrential Downpour program. This program has been described in testimony by one of its creators as follows:

> Torrential Downpour is a law enforcement surveillance software that is used exclusively by law enforcement. It is used to track, investigate, and eventually arrest those sharing child pornography through various P2P sharing networks…. Torrential Downpour is "somewhat unique" in that (1) it is designed to target and download files from a single IP address, as opposed to multiple sources, and restrict downloads to come from only that particular address (this is called a "single source download"): (2) Torrential Downpour creates a detailed log of events for evidentiary purposes; and (3) Torrential Downpour does not share files.

United States v. Maurek, 131 F. Supp. 3d 1258, 1261 (W.D. Ok. 2015). The indictment puts the use of this software squarely at issue by claiming that Mr. Schwier distributed child pornography when law enforcement downloaded child pornography from his computer or that he possessed child pornography when the software claimed it was he had it when in fact he did not. The government claims that Mr. Schwier's computer was the sole candidate for each download but acknowledges that BitTorrent software typically assembles a file from multiple sources.

In addition Mr. Schwier seeks disclosure of the "pooled information" that enabled the government to focus on the IP address later determined to be associated with Mr. Schwier.

Mr. Schwier also seeks copies of any license, training materials, user manuals, and instructions associated with the program, needed to effectively cross-examine the investigative officer and/or the government's expert as to their ability to use the program correctly and to testify about it. These materials may also aid in showing that the program was used in a manner that violated Mr. Schwier's rights.

The timing of the police investigation spanning October 2016 to April 2017 also strongly suggests there may have been times that police tried to download files and were unable to do so because sharing was precluded, either by features in the law enforcement software or for other reasons. Such evidence would tend to show that Mr. Schwier did not allow others to download from his computer. Such evidence is discoverable under *Brady* and should be disclosed.

Mr. Schwier also requests chain-of-custody documentation for any files the FBI claim to have downloaded, including but not limited all *meta*-data for any alleged downloaded file. Such documentation is a routine part of the impoundment process for digital evidence and should be provided.

CONCLUSION

Given the problems the FBI had successfully downloading and receiving any files, it is material to the defense of these charges to determine the actual origins of the file with the file designation 1180842565051.jpg. This file was not found on any digital media seized from Mr. Schwier's residence. At this time no known creation or access dates are known to exist for this file, and serious questions exist as to whether this file was ever on any media or device associated with Mr. Schwier. Given the manner in which BitTorrent normally works it is entirely possible this file did not come any device possessed by Mr. Schwier but rather was downloaded from another source. It is imperative that Mr. Schwier have access to the Torrential Downpour software to investigate this and to have access to the actual file as well for inspection and examination. Mr. Schwier has a constitutionally protected right to investigate the Government's claim that this file was downloaded from his computer. Production of the software and the file is essential to the defendant, and to properly preparing a defense and for proper cross-examination of the government's witnesses. Without such access

Mr. Schwier is denied the right to confront the evidence of which he is accused of possessing and distributing.

Respectfully, Mr. Schwier requests an order from the court compelling discovery and the production of the Torrential Downpour software.

DATED at Anchorage, Alaska, this 12th day of September 2019.

THE LAW OFFICES OF ROBERT HERZ, PC
s/ Robert M. Herz
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
Phone 907-277-7171 / Fax 907-277-0281
rmherz@gci.net
AK Bar No. 8706023

CERTIFICATE OF SERVICE
I hereby certify that on September 12, 2019, a copy of the foregoing C- Motion to Compel Discovery and Production of Evidence was served electronically on Assistant United States Attorney's Office s/ Robert Herz

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

DECLARATION OF JEFFREY M. FISCHBACH

I, Jeffrey M. Fischbach, declare as follows:

1. I am a computer forensics expert and founder of SecondWave, Inc. a firm specializing in digital forensics. My offices are located in Los Angeles, California. I am competent to testify and the matters contained herein are based on my own personal knowledge.

2. I am a board-recognized computer forensic examiner specializing in information, communication, stored data and electronic location technologies;

3. I have worked as an expert in this field for more than twenty-five years and have consulted on, and testified in municipal, Federal and military courts, both domestic and abroad, in dozens of cases involving digitally-recorded evidence, and offer my services to both Government and Defense;

4. I have been granted security clearance, and use of a Sensitive Compartmented Information Facility (SCIF) by the DOJ for the purposes listed above;

5. I routinely lecture and provide training in my area of expertise to civilian attorneys, law enforcement, and judges throughout North America, and my opinions have been cited, on record, by the United States Supreme Court;

6. I have conducted hundreds of forensics examinations on thousands of pieces of

evidence, including hard drives, cell phones, removable storage media, network data centers, and other electronic devices. My Curriculum Vitae is attached hereto.

7. I have provided expert forensic consultation in hundreds of criminal cases throughout the United States, the EU, Japan, Guam, and Rio de Janeiro, since the year 1997, and have testified dozens of times in State, Federal and Military Courts. I have qualified and testified as an Expert in numerous State and Federal Courts in the fields of forensic Data, Cellular Phones, Cellular Tower Coverage, RF Propagation Mapping, GPS Accuracy, Computers, Audio, Video, Data Analysis, and still Image Analysis. I have testified in numerous federal courts as an expert in Computer Forensics and Cellular Phone and Cellular Records analysis. I have worked as a defense expert on dozens of state and federal cases nationwide that were subject to Protective Orders and/or Non-Disclosure Agreements (NDA). I have never violated, nor have I been accused of violating any Protective Order or NDA. To the contrary, my services have been utilized by courts for the purposes of assisting in investigations of alleged misconduct by government agencies. I consult with law enforcement agencies whenever requested.

8. I have been retained as a computer forensics expert by Robert M. Herz, counsel for Mr. Matthew Schwier, for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this matter. I have reviewed discovery materials produced to the Mr. Schwier by the Department of Justice including, but not limited to seized and cloned hard drive, SD cardZ, and disc media, as follows:

a. Government Exhibits 1a, 1b & 1c, a pink folder with printed material enclosed;

b. Government Exhibit 2a, a pink folder with printed material enclosed; Item 2a appears to be a print-copy of 1B37, but contains no authenticating hash value or chain of custody documentation;

c. Government Exhibits 3a-3c, a pink folder with printed material enclosed;

d. Government Exhibits 4a & 4b, a pink folder with printed material enclosed;

e. Government Exhibits 5a-5e, a pink folder with printed material enclosed;

f. Government Exhibits 6a-6c, a pink folder with printed material enclosed;

g. 18-295-02A (CD-R), entitled "hashes";

h. 18-295-02A 1b33 A Mac Tower, with attached hard drive, containing forensic image files;

i. 18-295-02A 1b34 (CD-R), entitled "One CD with hash values containing CP found on comp…";

j. 18-295-02A Item 1b36, entitled "One CD containing Bit-Torrent session logs from 11/22/2016". Contains 2 duplicate folders found in 1B37: SD /2016-11-22_20-48-30_31/Download & /2016-11-22_20-48-30_31/Log;

k. 18-295-02A Item 1b37 (SD Card", entitled "One SD card containing FTK reports, file with hash values, BitTorrent session logs". Contains SD CARD Distribution/1180842565051.jpg. NO chain of custody provided, but torrent logs were (SD CARD BT Session/2016-11-22_20-48-30_31/Logs & SD CARD BT Session/2016-11-22_20-48-30_31/Download). Contains ZERO (0) byte files, duplicate provided on CD in Anchorage. 1B37 SD CARD also contains CP hashes [EMPTY FOLDER] & FTKReports, as previously provided;

l. 18-295-02A Item 5c (CD-R), entitled "Schwier CP hashes";

m. 18-295-02A Item 5c (CD-R), entitled "Schwier BT Session";

n. 18-295-02A Item 5c (Portable Hard Drive), entitled "Passport";

o. 18-295-02A Item 5c (SD Card), entitled "FTK reports, has values, bit torrent";

p. 18-295-02A Item 5c (DVD-R), entitled "Obscene Material, return to FBI";

9. It should be noted that almost every item listed above contained duplicate items, in part, or in whole, within other evidence provided. Although provided individual item identification, the actual volume of unique, non-duplicate evidence in this matter appears to be just a fraction of what appears in the itemized discovery.

10. According to discovery, this case originated on October 20, 2016 when the IP address 216.137.195.191, as identified by FBI SA Daryl Allison, was allegedly sharing files, which he identified as possible child pornography.

11. In order to understand the complexities of the undercover investigation that allegedly identified Mr. Schwier in this matter, it is imperative to understand the difference between the "BitTorrent network", a "torrent", an "info hash", a common web page, and an actual image or video that depicts child pornography.

12. The "BitTorrent network" is essentially a protocol, or set of rules that allows users

to download and/or upload parts of files between many different users for the purposes of reassembling the constituent parts into complete files. The process is analogous to an automobile manufacturer receiving parts of a vehicle from various sources. Minus any single part, the automobile may not be capable of being driven. This means that someone downloading files on the BitTorrent network may get small pieces of a file from many different computers in order to reassemble the complete file on their own computer. This also means that, as a single un-drivable portion of an automobile frame may contain an identifiable registered Vehicle Identification Number (VIN), a user with an empty file container or a small fragment of a file may still be identified on the BitTorrent network as a download candidate for the whole file, even if they don't possess the whole file.

13. The object behind this protocol is similar to automotive assembly line methods. It is to facilitate a fast delivery and assembly of a file, by "shipping" multiple parts simultaneously from numerous sources. As such, a file that might have taken hours to download from a single source, might only take minutes via a torrent network.

14. A "torrent" itself is simply a text file, proprietary to the BitTorrent network that contains instructions for torrent software, such as uTorrent or BitLord, which describes how to download a file or sets of files on the BitTorrent network. Torrent files do not contain content data, such as images or videos, but rather an index containing information about the files associated with that torrent including but not limited to, names of the files instructed to download, the torrent author, the date the author of the torrent created the file, the number of files the torrent is set to download, and the URLs tracking the torrent activity.

15. An "info hash" is a mathematical algorithm or hash value that uniquely identifies the "torrent" on the BitTorrent network. Although it has been described as synonymous with a fingerprint, the info hash only identifies the torrent itself, not the actual files the torrent would download if parsed.

16. If, for example, Person A downloads a torrent to his computer, the info hash and file names of every file associated with that torrent would be automatically saved (cached) to his computer. If that torrent is never parsed, the associated files are never

actually downloaded to the computer and Person A does not possess those files. However, that torrent may still be read by torrent software and falsely advertised on the BitTorrent network as a download candidate for all of the associated files, even if none of the files exist. Similarly, forensic software would be able to identify the *names* of those files, even though the files themselves had not been received. If Person B tries to download the same torrent on the BitTorrent network, Person A will be listed as a download candidate. However, the files downloaded to Person B's computer will not come from Person A, rather, the bits and pieces will come from other users on the BitTorrent network who actually have the files.

17. During my independent computer forensics examination of items seized from Mr. Schwier, I was not able to locate the torrent, the info hash or the files of child pornography identified during the undercover investigation. In addition, the torrent, the info hash and the files of child pornography were not found by the government's forensic examiner either. According to discovery, it appears that the information that a torrent containing files of child pornography was available at IP address 216.137.195.191 was actually obtained by automated law enforcement sensitive software that monitors peer-to-peer file sharing networks. That software was identified in discovery as Torrential Downpour.[1] "Torrential Downpour" is part of a larger Peer-to-Peer (P2P)

---

[1] See Government discovery Bates Stamped pages:

1. Bates 176-232 – 10/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 176) – "2016-10-20 01:33:56 - Torrential Downpour version 1.23"
2. Bates 233-238 – 10/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 233) – "<!-- Torrential Downpour download status -->"
3. Bates 240-267 – 10/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 240) – "2016-10-20 01:33:56 - Torrential Downpour version 1.23"
4. Bates 270-531 – 10/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 270) – "2016-10-20 02:14:05 - Torrential Downpour version 1.23"
5. Bates 532-536 – 10/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 532) – "<!-- Torrential Downpour download status -->"
6. Bates 540-635 – 10/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 540) – "2016-10-20 02:14:05 - Torrential Downpour version 1.23"
7. Bates 637-1901– 10/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 637) – "2016-10-20 03:46:41 - Torrential Downpour version 1.15" and "2016-10-20 03:46:42 - Torrential Downpour version 1.15"
8. Bates 1902-1915 - 10/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 1902) – "<!-- Torrential Downpour download status -->"
9. Bates 1920-1948 – 10/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 1920) – "2016-10-20 03:46:41 - Torrential Downpour version 1.15" and "2016-10-20 03:46:42 - Torrential Downpour version 1.15"

communications investigation toolset collection known as "RoundUp Suite". See, Liberatore, Levine, Wallach, Wolak & Kerle, 2015. As part of the RoundUp Suite, "Torrential Downpour" was apparently developed to enable single-source peer-to-peer file sharing between law enforcement and target computers potentially sharing contraband files or media. RoundUp Torrential Downpour is a specially modified version of a BitTorrent client. RoundUp Suite is available to law enforcement *only,* and is provided at no cost to eligible law enforcement entities. Liberatore, et al, 2015. As such, scientific peer review has not been conducted, as has been done in other investigative software, like AccessData's Forensic Toolkit (FTK), and Guidance Software's EnCase, that can be obtained and tested by individuals in the scientific (e.g., non-law-enforcement) community.

18. The foundational toolsets for what are now known as RoundUp Suite were the product of law enforcement agencies partnering with Oak Ridge National Laboratory in 2009, in an effort to automate investigative processes involving Peer-to-Peer networks. See, Borges et al 2011.

19. I have examined work product, and reviewed available online information about Torrential Downpour, and have read cases where the program was used and described. This information states that the program generates log files for use as evidence in

---

10. Bates 1950-7923 – 11/20/16 Details Log: "Torrential Downpour" appears at p. 1 (Bates 1950) – "2016-11-20 19:23:13 - Torrential Downpour version 1.15" and "2016-11-20 19:23:14 - Torrential Downpour version 1.15"

11. Bates 7924-7937 – 11/20/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 7924) – <!-- Torrential Downpour download status -->"

12. Bates 7954-7992 – 11/20/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 7954) – "2016-11-20 19:23:13 - Torrential Downpour version 1.15" and "2016-11-20 19:23:14 - Torrential Downpour version 1.15"

13. Bates 7994 – Data Written Log: "Torrential Downpour" appears – "<!-- Torrential Downpour data written information -->"

14. Bates 7996-8203 – 11/22/16 Download Status Log: "Torrential Downpour" appears at p. 1 (Bates 7996) – "<!-- Torrential Downpour status -->"

15. Bates 8207-8938 – 11/22/16 Summary Log: "Torrential Downpour" appears at p. 1 (Bates 8207) – "2016-11-22 20:48:30 - Torrential Downpour version 1.15" and "2016-11-22 20:48:3014 - Torrential Downpour version 1.15"

criminal trials. A key purpose of the Torrential Downpour software is to log and document efforts to download contraband from a target computer. According to the discovery provided, as well as repeated unanswered requests for authenticating documentation, the Government has produced in this case no uniquely-identifying device data beyond basic IP addresses associated with the defendant's wireless household network. In my opinion, and in the opinion of respected forensic investigators, comprehensive forensic investigations must include device-identifying data that exceeds basic IP address assignments from an Internet Service Provider (ISP), to include system level Globally Unique Identifier (GUID) logs.

20. In my examination of the government's case I have discovered that the investigator's claim to have accessed numerous files which could not be downloaded. According to the BitTorrent protocol, the only reason a file could not be downloaded is because either no content exists on the queried system, or because that file was not being shared by the user. In the instant case, the investigator identifies numerous files which he says he was unable to download. It is my opinion, given what I know of the BitTorrent protocols, that either the investigator is mistaken, the software was operating in error, or the software has been modified in such a way as to exploit vulnerabilities in the protocols, and force the client to exceed the limitations of the BitTorrent protocol, thus "hacking" the source for evidence of files not intended to be shared.

21. It is well-known, and confirmed, that prior versions of popular BitTorrent client software, including uTorrent, contained serious remote exploits that have since been acknowledged and patched in current versions. (See, BitTorrent Bootstrap 'lazy_bdecode.cpp' Remote Code Execution Vulnerability, Symantec Corporation [US]: Security Focus.https://www.securityfocus.com/bid/70812/discuss). These vulnerabilities allow the client computer to be manipulated remotely, without the user's knowledge.

22. Given Torrential Downpour's alleged ability to "see" files that appear not to be available for download, it seems very likely that the application leveraged a BitTorrent Remote Code Execution vulnerability to allow law enforcement investigators to control the file sharing settings on the suspect devices remotely. Descriptors listed in various

vulnerabilities indicate that use of the exploit could in fact be used to execute code that, by extension, could then modify user settings in an application's sharing permissions. Whether or not a particular vulnerability was exploited, it has been reported in a number of cases that Torrential Downpour may be exploiting vulnerabilities in the Torrent client allowing law enforcement access to files not meant to be publicly shared. A defense examination of the Torrential Downpour software can confirm or deny the use of any BitTorrent vulnerability exploits. Defense experts, in my opinion, should be allowed to examine, under controlled and protected conditions, any and all logs, including system level GUID logs, associated with the investigation of the defendant's internet communications activities as well as the program itself and its user materials.

23. Having examined numerous P2P cases, and from personally observing the testimony of law enforcement personnel on similar cases, serious concerns have been raised regarding "quarantined" or proprietary law enforcement software that has not been subject to peer review, including Torrential Downpour, questioning the software's accuracy and reliability and whether the software is going beyond the scope of "publicly available" information. To my knowledge, as of the writing of this Declaration, this software has never been formally tested and/or validated by anyone and is unavailable for testing by any third-parties.

24. In my experience, it is critical to the defense of Mr. Schwier's case to understand how this software functions in order to determine its reliability and accuracy in identifying files reported as "publicly available" from Mr. Schwier's computer. In addition, forensic review of the Torrential Downpour software may enable the defense to show that the program had capabilities beyond those claimed or acknowledged by law enforcement. This evidence may help the defense demonstrate how law enforcement was able, using the software, to access files on defendant's devices that were apparently inaccessible for download by either specialized law enforcement tools, or by members of the general public. In a measurable way, such capabilities could be had by exploiting [subsequently patched] BitTorrent client software vulnerabilities, and changing or overriding user settings to allow police to access files defendant had intended to keep

private, by searching for files in places defendant had intended to block from access to other Bit Torrent users, or by downloading only fragments of files, rather than complete files.

25. Furthermore, Mr. Herz has requested my assistance in preparing cross-examination of a government witness who will testify about his use of Torrential Downpour as *the* culminating basis of his investigation of Mr. Schwier. Without access to this software, I can neither confirm the technical accuracy of the witnesses' testimony, nor can I competently prepare defense counsel to cross-examine the witness.

26. Thus, the implication in this case is that the software may be identifying files of suspect child pornography as being on Schwier's computer that in fact are not there or are not "publicly available" and were not intended to be shared. Since the Torrential Downpour software has never been independently tested and validated it is critical to Mr. Schwier's defense to understand how this software functions in order to determine its reliability and accuracy in identifying files allegedly belonging to Mr. Schwier. This is especially so when none of the files, the torrent or the info hash were found on any of his computers. Again, to my knowledge, no publicly available study has been undertaken to ascertain the reliability of the data produced and reported by the Torrential Downpour software.

27. In my quarter-century of forensic experience, much of which comes from examining, following, and teaching acceptable scientific and law enforcement practices, it is not acceptable science to rely on a tool (software) that has not been tested and subjected to peer-review. Even less-so when a tool is barred from peer review. This is why most forensic examiners use tools like EnCase and FTK, because they are industry standard tools that are available for testing and validation by anyone and, as such, have been accepted by the Courts as viable tools. However, even those tools have been proven to produce inaccurate and unreliable data at times which has only been discovered through the ability to test and validate them, leading to critical patches in the software.

28. The biggest challenge with developing an accurate tool is the diversity of hardware data being collected and analyzed. This is why even tools like EnCase and FTK

sometimes produce inaccurate and unreliable results. No two computer systems are identical. Computers are installed with different operating systems and there are hundreds of different versions of the same operating system, some are updated regularly and some are not updated at all. Those operating systems have thousands of different settings that can make each system unique in how it functions and records data. Within those operating systems a user can install millions of different software applications from large commercially produced software to small home-made software applications. Software applications may have bugs; data can be corrupted or incomplete; computers can be infected with viruses, Trojans and other malware. All of these variables have an effect on how that data is collected, analyzed and documented by a tool. While a tool may provide accurate information on an updated Windows system without any malware, the same tool may yield false results on a system that has not been updated and is infested with viruses.

29. When talking specifically about peer-to peer (P2P) software, there are hundreds of versions of file sharing software applications that users can download from the Internet. Some are free and some are paid. Some are updated regularly with new versions, some are not. Some of those applications are open source, meaning the user can actually modify the source code of the application allowing it to function differently than the exact same piece of software installed on another computer. I have personally been researching, testing and analyzing P2P file sharing software available to the public for over ten years including, but not limited to, LimeWire, FrostWire, Bearshare, Ares, BitTorrent, eMule, Phex and Shareaza. What I have discovered in all of these programs is that they can contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable. In that regard, any tool used to collect, analyze and document data associated with these applications may also be inaccurate and unreliable.

30. For all of the reasons stated above, and under general scientific principles, it is my opinion that the software relied upon during the undercover investigation needs to be tested and validated by a qualified third-party to determine its functionality, accuracy and reliability.

31. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, and I hereby reserve the right to amend any statement should additional information be made available to me at a later date.

DATED at Los Angeles, California, this 12th day of September 2019.

Jeffrey M. Fischbach

Curriculum Vitae

Robert William Erdely
Pennsylvania State Police (retired)
244 McHenry Road
Indiana, Pa. 15701

Certifications

2009	Access Data Certified Forensic Examiner
2009	Certified at the Federal Law Enforcement Training Center, Seized Computer Evidence Recovery Specialist
2007	Certified Forensic Computer Examiner, International Association of Investigative Specialists
2004	Certified Cisco Internetwork Professional
2004	Certified Information Systems Security (INFOSEC) Professional.
2004	Certified Cisco Security Professional.
2004	Certified by ISC2 as a Certified Information Systems Security Professional (CISSP®)
2003	CompTIA A+ Certified Professional.
2003	Certified a Microsoft Database Administrator
2003	Certified as a Microsoft Systems Engineer for Windows 2003
2003	Certified as a Microsoft Systems Engineer: Security
2003	CompTIA i-Net+ Certified Professional.
2003	CompTIA Network+ Certified Professional.
2003	Certified Cisco Design Professional.
2002	EnCase Certified Examiner
2001	Cisco Certified Network Professional.
2001	Certified as a Microsoft Systems Engineer for Windows 2000
1999	Certified as an Electronic Evidence Collection Specialist, International Association of Computer Investigative Specialists

Professional Activities

2010-2016	Member of Interpol's Technical Working Group which is currently working with Law Enforcement and Universities to develop tools to investigate the exploitation of children on the internet.
2010-Present	Instructor for both the International Centre for Missing and Exploited Children and Fox Valley Technical College
2009-Present	Developed a system to investigate the sharing of child pornography on the internet.. This information is used by law enforcement in over 60 countries to locate, investigate and prosecute these child predators. This system has resulted in the initiation of more than 15,000 investigations and rescuing countless child victims.
2007-Present	Instructor for the Internet Crimes Against Children (ICAC). Instruct online Investigations, including Peer-to-Peer file sharing networks.

Experience

2012-Present	Detective with the Indiana County District Attorney's Office, Indiana County Pennsylvania. Assigned to investigate child exploitation investigations. I am currently assigned to the FBI Innocent Images Task Force, Pittsburgh, Pennsylvania.

2008-2012	Supervisor for the Pennsylvania State Police (PSP) Computer Crime Unit, Harrisburg, PA. Supervised both the investigative and digital forensic sections of the PSP.
2003-2008	Supervisor of the Southwest Computer Crime Task Force comprised of State and Local Law Enforcement.
1998-2003	Assigned to Bureau of Criminal Investigations, Computer Crime Unit. Responsible for all aspects of proactive and reactive investigations, including evidence duplication, documentation and examination, regarding criminal activities utilizing technology to facilitate the illegal activities.
1997-2007	Senior Computer Network Administrator for an Internet Service Provider, providing service to over 3000 users
1999-2004	Instructor for the Pennsylvania Chiefs of Police Association for Federal, State and Municipal Police Officers along with representatives of the Attorney General and the District Attorneys regarding computer forensic examination processes and procedures and the online investigation of computer crime.
January 2003	Speaker at the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network's (MAGLOCLEN) Internet Investigation training Conference.
October 2001	Speaker at the Pennsylvania District Attorneys Institute's Computer Crimes Training course.
1994-1998	Assigned to PSP Vice Unit, Troop A
1992-1994	Assigned to Patrol Unit, PSP, Indiana, PA.

Education and Training

1989	Community College of the Air Force
1990	Edinboro University of Pennsylvania
1992	Graduated from the Pennsylvania State Police Academy
1994	Drug Investigators Course
1995	Narcotics in the mail, Interdiction and Clandestine Labs seminar, U.S. Department of Justice
1995	Investigation of Computer Crime, National White Collar Crime Center
1996	Vice Investigations Seminar
1996	Eastern States vice Investigator training Conference
1997	High risk Warrant Service Training
1997	Gambling Device Examination Training
1997	Top Gun, Undercover Drug Law Enforcement Training
1997	Certified to Utilize Electronic Surveillance (Wiretap)
1999	Investigation of Computer Crime, International Association of Chiefs of Police
1999	Investigation of Computer Crime, SEARCH, the National Consortium for Justice Information and Statistics
1999	Unix investigators course at FBI Academy
2001	Guidance Forensic Software Intermediate Course
2001	Guidance Forensic Software Advanced Course
2002	16 hour Windows 2000 Security seminar by Computer Security Institute at FBI Pittsburgh
2002	Fundamentals of Incident Handling course at the CERT Coordination Center (Incident Handling for Computer Emergency Response Teams).
2002	High Technology Crime Investigation Conference
2002	Advanced Data Recovery and Analysis, National White Collar Crime Center
2004	Advanced Solaris Administration Course by FBI
2004	FBI Symposium on Online Child Pornography/Child Exploitation
2005	National White Collar Crime Center's Advanced Data Recovery and Analysis course
2005	Attended NTI Forensic Examination training

2006 Department of Defense Cyber Crime Conference
2006 Sun Educational Service course "Securing Solaris & Network Intrusion Detection"

Publications

Forensic Investigation of Peer-to-Peer File Sharing Networks.
DFRWS Annual Digital Forensics Research Conference, August 2010

Certified Expert

- Certified as a computer expert including online investigations by the United States District Court, Western District of Pennsylvania, in United States vs. Abraham (2006)
- Certified as a computer forensic expert by the United States District Court, Eastern District of Pennsylvania, in United States vs. Schade (2008).
- Certified as a computer expert including online investigations in Middle District of Pennsylvania, United States vs. Doyle. (2011)
- Certified as a computer forensic examiner and in internet investigations in the Eastern District of Pennsylvania, United States vs. Fitzgerald Horton (2013)
- Certified as an expert in the case State of New Jersey v. Julio Gomez-Marte (2015)
- Certified as a computer forensic examiner and in internet investigations US District Court Maryland, US vs. Carl Javan Ross (2016)
- Certified as a computer forensic examiner and in internet investigations State of New Mexico vs. Jeffrey Morrill (2016)
- Testified as an expert in the BitTorrent file sharing network. US v Larry O'Neal US District Court Bangor Maine (2019)
- Testified as a file sharing expert in US v Matthew Lee Lane Eastern District of Washington State

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

Validation Report

This document will explain the testing procedure and methodology used to validate the Torrential Downpour v 1.22 investigative tool. Understanding the following terms[1] will be helpful when reading this document as many of them will be mentioned throughout.

A. GLOSSARY

availability
The number of complete copies of the torrent contents there are distributed in the part of the swarm you're connected to. The amount of the torrent contents you currently have is included in the availability count. A swarm with no seed and with an availability below 1.0 will likely be unable to finish transferring the complete torrent contents.

byte
A unit used for measuring the size of data on a computer storage device. Many people confuse "byte" for "bit" when referring to speeds. A byte is composed of 8 bits, so there is a clear distinction, and terminology should not be confused when referring to bytes.

client
The application a user is using when connected to a swarm. In this case, the application being used to connect to swarms is BitTorrent, so it is the client.

download
The act of transferring data from another computer onto your own.

firewall
A barrier (hardware and/or software) that prevents communication to and/or from certain computers, depending on the rules set in the firewall.

hash
A "fingerprint" of data assumed to be unique to the data. Because of the assumed uniqueness of the data, it is used to verify that a piece of data is indeed uncorrupted (since the corrupted data's hash would not match its expected hash).

hash check
The comparing of a piece of data's hash with a reference hash in order to verify the integrity of the piece of data.

hashfail
When a piece fails the hash check used to verify data integrity.

[1] This excerpt of definitions of terms was taken directly from the BitTorrent website. These definitions as well as a full list can be found at http://help.bittorrent.com/customer/portal/articles/179175-glossary.

interested

This word describes the state of a BitTorrent connection. When a peer is interested, it means the peer is interested in the data that the peer on the other end of the connection has and is willing to accept data from the other peer.

IP address

A number used to uniquely identify devices on a network.

LAN IP address (also referred to as a private IP)

The private, internal IP address that locates a computer on a LAN. A LAN IP address is not visible to users outside of the LAN. As described by RFC 1918, the following ranges are designated as reserved IP addresses for private LANs:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

P2P (peer-to-peer)

The use of bandwidth of users using the same peer-to-peer service to perform the functions of the peer-to-peer service or software. Centralized servers are not what keeps P2P networks alive, but rather, the peers themselves.

payload

The actual data being transferred from sender to receiver, not counting overhead.

peer

A user/client connected to the swarm. People sometimes refer to peers as "leechers," though they also use the same word to refer to its more negative connotation. It's recommended that you use the word "leecher" to strictly refer to people who don't share so to keep the distinction clear and confusion to a minimum.

piece

The smallest appreciable unit of data in BitTorrent. The size of pieces can be different depending on the .torrent file in question.

protocol

A set of rules and description of how to do things. In the case of the BitTorrent protocol, it is a set of rules describing how BitTorrent clients should communicate and transfer data with each other.

seed

A peer with 100% of the data in the torrent contents.

seeding

The act of being connected to a swarm as a seed.

swarm
The collective group of peers (which includes seeds) that are connected by a common .torrent file.

torrent
A small file containing metadata from the files it is describing. In other contexts, it is sometimes used to refer to the swarm connected around that small file.

upload
The act of transferring data from your computer onto another.

B. SETUP: Note that all software was installed using default setting, except where otherwise noted.

1) Both the investigative system and the target system were created using VMWare Workstation Player 15 version 15 build-10952284. This free tool, downloaded from https://www.vmware.com, allows for the creation of virtual machines (VMs), which can easily be copied or transferred to other users or systems. As taken from the VMWare website:

"The isolation and sandbox capabilities of VMware Workstation Player make it the perfect tool to help you learn about operating systems, applications and how they work. Being able to run a server environment on a desktop PC also allows you to explore software and application development in a "real world" environment without interfering with the host desktop.' [2]

2) Windows 10 Pro (64 bit) build 1809 OS Build 17763.253 was chosen as the operating system for both VM's. Prior to conducting the validation test, Microsoft automatic updates was disabled on both machines. While Torrential Downpour will run on older versions of Windows, Windows 10 was selected as it is the most recent release of the Windows operating system. Torrential Downpour does not operate on other operating systems such as Linux or Mac iOS devices.

3) Private Internet Access (PIA) version .81 was used on both VMs. PIA allows for internet connectivity through a virtual private network (VPN):

"*PRIVATE INTERNET ACCESS provides state of the art, multi-layered security with advanced privacy protection using VPN tunneling. Scroll below to the Security Layers section to learn more about each individual layer.*

Our services have been designed from the ground up to be able to operate using built-in technology pre-existing in your computer or smartphone device.

[2] Quoted from the VMWare website at https://www.vmware.com/products/workstation-player.html

The services operate at the TCP/IP interface level, which means all of your applications will be secured, not just your web browser." [3]

4) In order to conduct packet captures to show network traffic, the software tool Wireshark version 2.6.6 was used on both VM's. This free tool is available for download from https://www.wireshark.org/ Wireshark is used to record network traffic (packet captures) on the target machine to show how a standard BitTorrent client, in this case BitTorrent, conducts multisource downloads to obtain a payload. When utilizing Torrential Downpour, Wireshark is used on both the investigative and target VMs to show that the software only conducts single source downloads (SSD).

"Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.' [4]

Bram Cohen, the architect of the BitTorrent protocol, recommends the use of Wireshark to test BitTorrent applications:

"When developing a new implementation the Wireshark protocol analyzer and its dissectors for bittorrent can be useful to debug and compare with existing ones." [5]

5) To display hash values of created or downloaded files, the program Cyohash version 1.02 was utilized on both VM's. This tool adds right click functionality to the mouse that allows for hash values to be easily calculated and displayed for individual files. This tool will calculate both the MD5 and SHA1 hash values for a given file.

6) For this validation test, a .torrent file needed to be created to share non-copywritten files on the BitTorrent network. To create this .torrent and to download and share (seed) these files, BitTorrent 7.0 was used.

7) The images used in the creation of the validation torrent were downloaded from https://www.pexels.com/:

"It's hard to understand complex licenses that is why all photos on Pexels are licensed under the ***Creative Commons Zero (CC0) license****. This means the pictures are completely free to be used* ***for any legal purpose****.*

- *The pictures are* ***free for personal and even for commercial use****.*

[3] Quoted from the PIA website at https://www.privateinternetaccess.com/
[4] Quoted from the Wireshark website at https://www.wireshark.org/
[5] Bram Cohen, The BitTorrent Protocol Specification

- *You can modify, copy and distribute the photos.*
- *All without asking for permission or setting a link to the source. So,* ***attribution is not required****.*

The only restriction is that identifiable people may not appear in a bad light or in a way that they may find offensive, unless they give their consent. You should also make sure the depicted content (people, logos, private property, etc.) is suitable for your application and doesn't infringe any rights.

The CC0 license was released by the non-profit organization Creative Commons (CC). Get more information about Creative Commons images and the license on the official license page." [6]

Files of various sizes were used for the payload and were saved in a folder named "Validation stock photos". From there the pictures were arranged randomly in two separate sub directories named "1" and "2" respectively, with one file being left in the root directory. To create the .torrent file itself, the built-in creation tool incorporated into BitTorrent was pointed at the "Validation stock photos" folder. The piece size selected was 1024 kB and a number of trackers were added. No other options were changed.

8) For the investigative VM only, Roundup Torrential Downpour version 1.22 (TD) was used. This investigative software is available for law enforcement only and was developed by the University of Massachusetts, Amherst. TD follows the BitTorrent protocol with few exceptions. The first exception is that TD does not take advantage of what is referred to as file swarming. File swarming can speed up the download process by downloading from multiple BitTorrent programs simultaneously. Instead, TD only requests to download pieces from a single IP thereby insuring that any downloaded data came from a single sharing BitTorrent program. Although standard BitTorrent programs will download data from a single IP address if that is the only download candidate available at that moment, TD can *only* download from a single IP address regardless of the number of BitTorrent programs sharing the same data. Secondly, TD cannot share data back to the BitTorrent filesharing network. This is easily accomplished since every piece of data we become in possession of was downloaded from a single IP who would never need those pieces back.

9) To view the contents of a .torrent file Roundup Torrent Viewer version 2.3, which is a standalone torrent viewing program, was used on both virtual machines. This program, which was written by the University of Massachusetts, Amherst, reads the data from a .torrent file and presents it in an easy to read format for the user. When directed at a .torrent file, the viewer will display information found within the torrent, which includes the following:

[6] Quoted from the Pexels website at https://www.pexels.com/photo-license/

- Info Hash
- Number of Pieces
- Files
- Creation Date (GMT)
- Publisher
- Public / Private
- Comment
- Piece Size
- Total Size
- Created By
- Publisher URL
- Files
    - File Name
    - Index Number
    - Size
    - Piece Range
    - Path
- Piece Hashes
- Announce / Announce List
- DHT Nodes

10) LibreOffice 6.1.3.2 was used for documentation purposes as it is also a free program which runs on multiple operating systems. It is available for download from https://www.libreoffice.org/

11) For consistent date and time documentation, the Atomic Clock application written by Timo Partl was downloaded through the Microsoft store and installed on both VMs. Information on Timo Partl can be found at https://timopartl.com/

12) To capture and record the entire validation process, Camtasia Studio 8 version 8.6.0 (paid version) was used https://www.techsmith.com/ . During the validation process the recording was conducted in real time and neither the recording of the investigative or target virtual machines was paused or stopped at any time.

C. <u>METHODOLOGY</u> This validation test was conducted on 01/23/2019. Times listed are Eastern Standard Time (EST).

1) Both the investigative and target virtual machines are started, and the atomic clock program run and placed in the bottom right corner of the screen. Both atomic clocks are compared to verify they are reporting the same time.
2) PIA started on both machines and connected to a location which allows for port forwarding.
3) **11:24 AM** Screen recording software started for target VM.
4) **11:24 AM** Private IP address of ethernet adapter displayed utilizing the Windows command prompt and ipconfig command. Private IP address is documented.

5) **11:24 AM** Public IP address for the target VM was displayed by going to the website www.IPChicken.com compared to the public IP reported by PIA. Public IP address and port is documented.
6) **11:25 AM** Validation .torrent file is opened in Roundup Torrent Viewer, and all information is displayed.
7) **11:25 AM** The Wireshark program is run and a packet capture recording of the network traffic is started. The Wireshark recording records all the communication in and out of the target VM. Analysis of this network traffic can be used to identify the communication, and confirm the download was available and conducted through connections with multiple sources as is typical when the data is available from multiple sources. To validate that TD conducts a download from a single BitTorrent program, rather than swarming, would be meaningless if the data was only available from a single BitTorrent program. This validation confirms that even though multiple sources for this data existed, TD will conduct a download from a single IP address.
8) **11:25 AM** BitTorrent is started, however no .torrent files are currently loaded into the program. The port number being used by BitTorrent is shown under the preferences of the program. This port number is the same as what is reported by PIA. The option to "Close button closes uT to tray" is disabled.
9) **11:26 AM** A standard download is initiated with BitTorrent by loading the .torrent file into the program. During the course of the download, the peers tab is displayed to show simultaneous active connections to multiple peers (swarming). This step documents that the data is available from multiple sources.
10) **11:28 AM** Once the payload for the validation torrent is completely downloaded and is displayed as seeding within BitTorrent, the Wireshark capture is terminated and saved onto the desktop of the VM. This packet capture is hashed and displayed using Cyohash. This step was conducted so that any expert will be able to confirm this is an accurate copy of the network traffic recording.
11) **11:28 AM** The .torrent file information is displayed from within the BitTorrent program by clicking on the bottom "General" and "Files" tabs. This data can be compared to the data previously displayed by the Torrent Viewer Program.
12) **11:28 AM** From within BitTorrent, the downloaded files referenced by the .torrent file are displayed. This is done by right clicking on the entry and selecting "Open Containing Folder". The names, sizes and hash values of each file are shown.
13) **11:30 AM** Screen recording the investigative VM is started.
14) **11:30 AM** Private IP address of ethernet adapter displayed utilizing the Windows command prompt and ipconfig command. Private IP address is documented.
15) **11:30 AM** Public IP address for the target VM was displayed by going to the website www.IPChicken.com compared to the public IP reported by PIA. Public IP address and port is documented.
16) **11:30 AM** Validation .torrent file is opened in Roundup Torrent Viewer, and all information is displayed.

17) **11:31 AM** The Wireshark program is run, and a packet capture recording of the network traffic is started on the investigative VM. The Wireshark recording records all the communication in and out of the investigative VM. Analysis of this network traffic can be used to identify the communication, and confirm the download was available and conducted through a connection with only a single source, even though the download was available from multiple sources as seen above in step 9.
18) **11:31 AM** A second Wireshark recording of the network traffic is started on the target VM. This second recording serves to document the investigative download made by TD. Analysis of this Wireshark recording can be used to confirm that all the data being referenced by this .torrent was shared to the investigative computer.
19) **11:32 AM** From within BitTorrent on the target VM, the .torrent being seeded[7] is highlighted and the bottom "Peers" tab selected. This is done to display any connections between this BitTorrent client and other BitTorrent clients which are communicating about and /or downloading pieces of this .torrent.
20) **11:32 AM** TD program is run, and an investigative download is initiated by loading the .torrent and specifying the IP address and port to connect to. Although this method of initiating an investigation is somewhat manual, TD has the ability to load these investigations into the program and conduct downloads automatically. This can be achieved by specifying an IP address, a range of IP addresses, or a geographic region. To determine the approximate location, TD utilizes the free geolocation database provided by www.maxmind.com. Regardless of the method used to initiate the investigation, only three pieces of information is used by TD: the .torrent identifier (infohash), the IP address and the port.
21) **11:32 AM** The date and time of the single source download is documented for both the target and UC VMs.
22) **11:32 – 11:33 AM** Once the single source download has completed, the Wireshark captures are stopped on both machines and saved to their respective desktops. Cyohash is used to display the hash values of these captures on both machines. This step was conducted so that any expert will be able to confirm this is an accurate copy of the network traffic recordings.
23) **11:33 AM – 11:43 AM** The validation worksheet on the investigative VM is completed. While completing the worksheet, the various log files are displayed as well as the specific file information such as file names, sizes and hash values. These can be compared to the data displayed in the Torrent Viewer Program as well as the information that was displayed on the target VM.
24) **11:40 AM** On the target VM the downloaded Validation stock photos folder is copied onto the desktop. A new .torrent file named "New Torrent" is created using this copied folder. This new .torrent is viewed in the torrent viewer program and verified as having the same infohash as the original torrent.
25) **11:42 AM** On the target VM, the copied "Validation stock photos" folder located on the desktop is renamed to "Validation stock".

[7] Peers possessing all the pieces of a .torrent that continue sharing that content are referred to as a seed. As a seed, the BitTorrent application will typically connect to other peers in order to share pieces of a .torrent.

26) **11:42 AM** A new .torrent file named “Name Change” is created using the newly renamed “Validation stock” folder. Once created, this new torrent is viewed in the torrent viewer program and shown to calculate a completely different infohash. This is done to show that any changes made to the file names, directories, data etc. will create a completely new .torrent. BitTorrent programs can only communicate and / or share with each other when both programs are communicating about a .torrent with the se infohash.
27) **11:43 AM** The validation worksheet is saved and closed and cyohash is used to display the hash values of the worksheet.
28) **11:44 AM** A third Wireshark capture of the network traffic is started on the target VM.
29) **11:44 AM** A second Wireshark capture of the network traffic is started on the UC VM
30) **11:44 AM** On the target VM, the original containing folder for the seeding .torrent (found in the “Downloads” directory) is opened and the top-level directory “Validation stock photos” is renamed to “Validation stock” and BitTorrent is shown to still be displaying the “seeding” message.
31) **11:45 AM** Another investigative download of the .torrent from the target VM is attempted.
32) **11:45 – 11:46 AM** BitTorrent seeding failure message displayed on target machine. Upon failure, the Wireshark captures on both VMs are terminated and saved to desktop. Both captures are hashed using Cyohash. This step was conducted so that any expert will be able to confirm this is an accurate copy of the network traffic recordings. The purpose of this step is to illustrate that when changes are made to any data referenced by the .torrent at the location where it is shared from, the BitTorrent program quickly recognized the change and therefore stops the seeding (sharing) process.
33) **11:46 AM** The top-level directory “Validation stock” is renamed back to its original name of “Validation stock photos”. BitTorrent is shown to still be displaying the error message from step 34. The Validation stock photos torrent is selected within the program and the option to “Start” is selected. The error message is shown to change to “Seeding”.
34) **11:46 AM** A fourth Wireshark recording of the network traffic is started on the target VM.
35) **11:47 AM** While BitTorrent is sharing the data, the folder containing the data is moved to a different location (desktop) and BitTorrent is shown to still be “seeding” the files. The purpose of this step is to illustrate that when any data referenced by the .torrent at the location where it is shared from is moved from that shared location, the BitTorrent program quickly recognized the change and therefore stops the seeding (sharing) process.
36) **11:48 AM** A third Wireshark recording of the network traffic is started on the UC VM.
37) **11:48 AM** Another investigative download of the .torrent from the target VM is attempted.
38) **11:48 – 11:49 AM** BitTorrent seeding failure message displayed on target machine. Upon failure, the Wireshark recordings on both VMs are terminated and saved to desktop. Both captures are hashed using Cyohash. This step illustrates what was described in step 35 above
39) **11:49 – 11:50 AM** The recordings for both VMs are terminated.

D. CONCLUSIONS

1. TD properly performed an investigative download from a single sharing BitTorrent program, which can be verified through the Wireshark recordings.
2. TD did not share any file data with any other BitTorrent program on the BitTorrent file sharing network.
3. Downloads can only occur when the data remains available in the location where it is being shared from.
4. Data can only be shared when the file(s) and/or directory(s) remained unchanged.
5. Downloads can only occur when two BitTorrent programs are communicating about the same .torrent (having identical infohashes).
6. Understanding the method by which BitTorrent shares data, that being that a .torrent file is a requirement to download any data, the download of unshared files is impossible.
7. All communications to and from the investigative computer were documented with a Wireshark recording (packet capture). Any nefarious activity where Torrential Downpour would send non- standard BitTorrent protocol messages would be exposed in the review of these packet captures.
8. Dates and times are properly recorded in the log files created by the software.
9. The infohash is properly recorded in the log files created by the software.
10. The IP address and port being investigated is properly recorded in the log files created by the software.
11. The IP address of the investigating computer is properly recorded in the log files created by the software
12. Files(s) and paths are properly recorded in the log files created by the software and match what is defined by the .torrent.
13. The data downloaded matched the data being shared on the target computer.
14. Data can only be downloaded while it is being shared by the BitTorrent program. If the data is moved or deleted it immediately ceases.
15. When a change is made to the shared data, even something as minor as renaming a file, the sharing BitTorrent application quickly recognizes the change and stops sharing the data.

E. POST TEST

1) At the conclusion of the validation video, Cyohash was used to hash the original recording files for both the investigative VM (Image 1) and the target VM (Image 2).

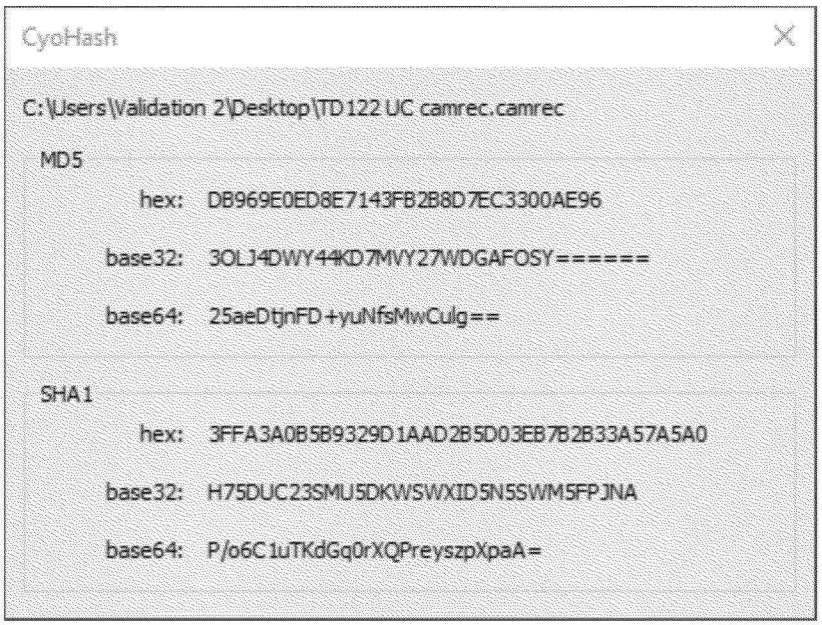

Image 1 Hash values of recording file of investigative VM

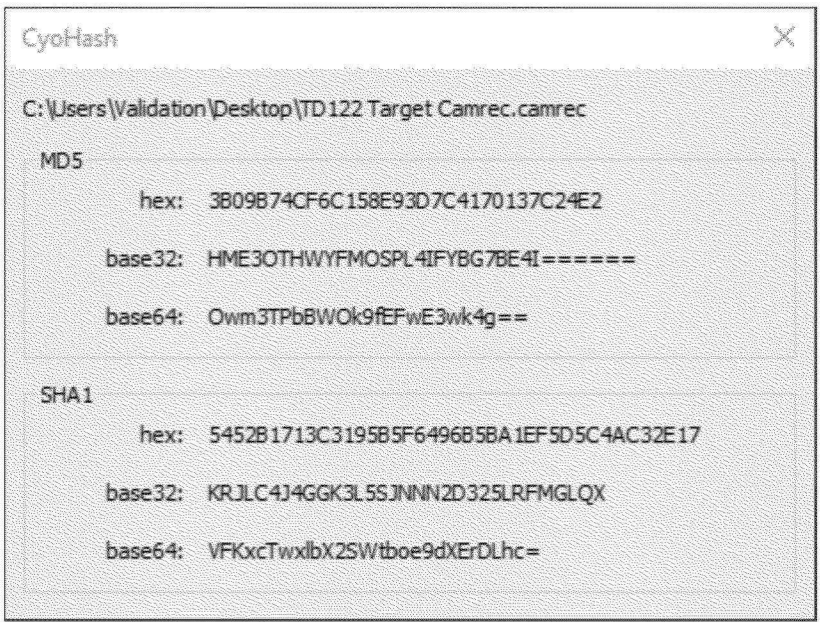

Image 2 Hash values of recording file of target VM

2) Both recording files were then compressed into a .zip format using 7-Zip, and hash values were calculated and documented for these .zip files (images 3 and 4).

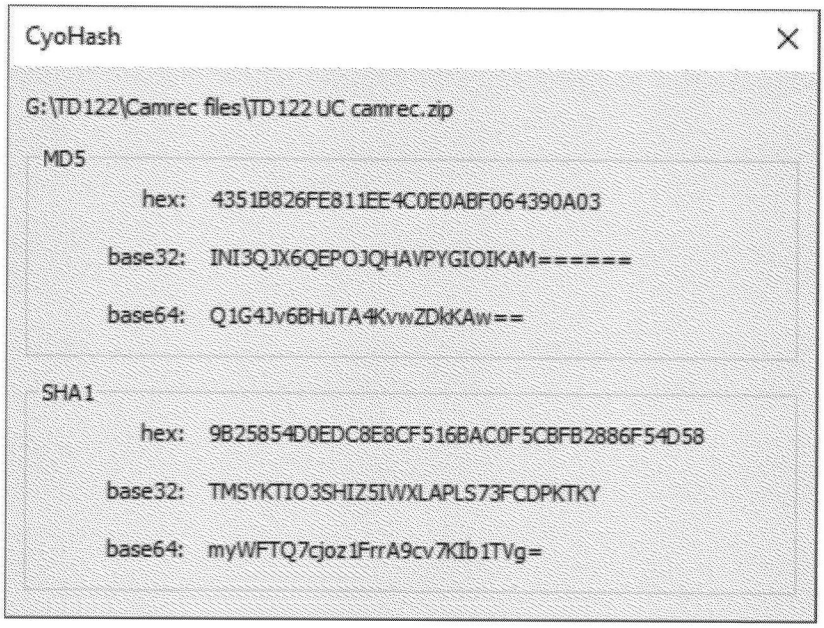

Image 3 Hash values of compressed investigative VM recording

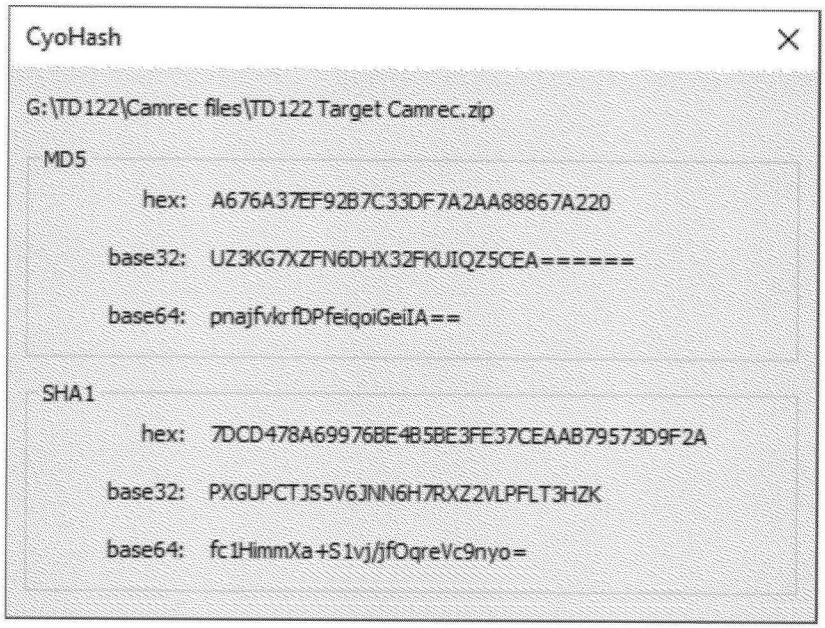

Image 4 Hash values of compressed target VM recording

3) The validation .torrent file, Validation stock pictures folder, and the validation worksheet were transferred from both the investigative VM and target VM to a containing folder outside of the VM's. This containing folder was compressed into a .zip format using 7-Zip and a hash value calculated and documented for the .zip file using Cyohash (Image 5).

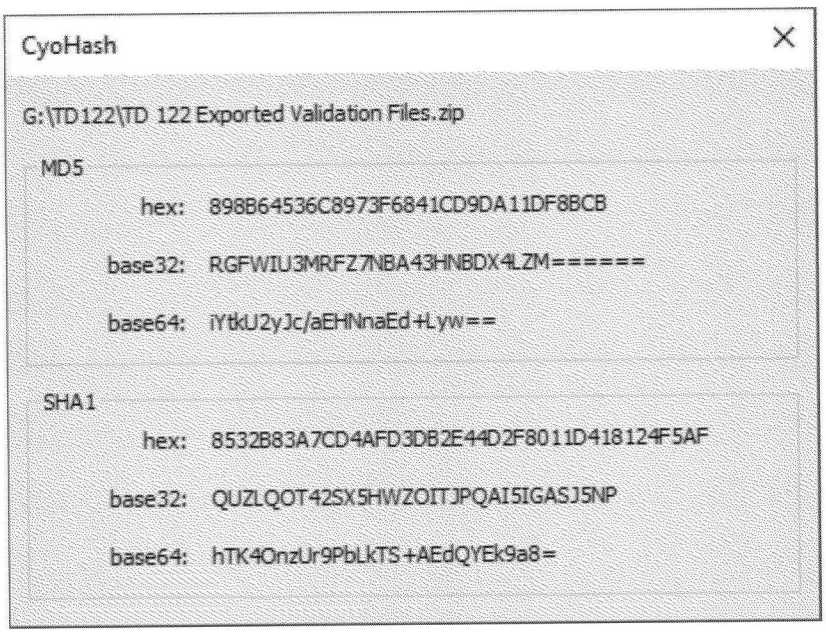

Image 5 Hash values of the exported validation files from both UC and target VMs

4) The Wireshark captures were transferred from both the investigative VM and the target VM into a containing folder outside of the VMs. Once all files were successfully copied the folder was compressed into a password protected .zip file using 7-zip and a hash value was calculated and documented (Images 6). The password used for this .zip file will be included in a separate document.

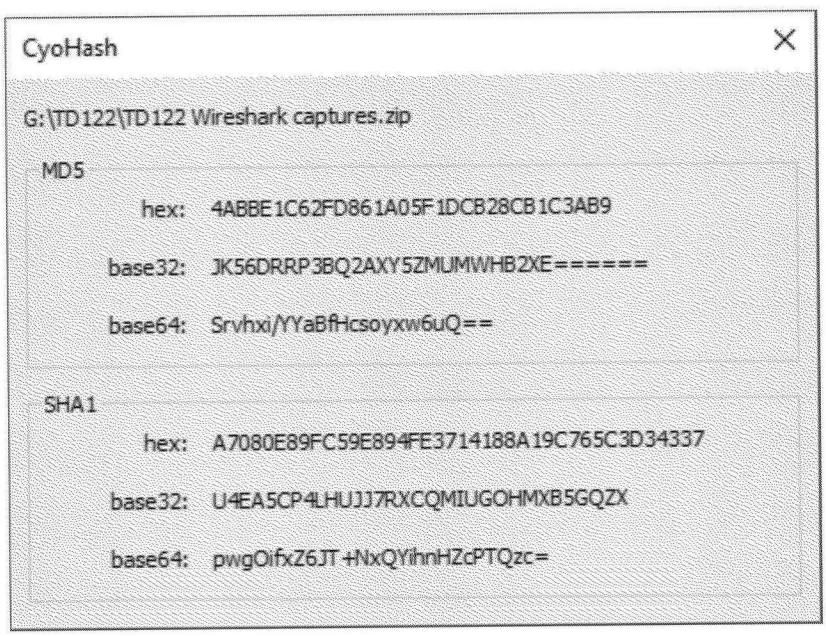

Image 6 Hash values of compressed Wireshark captures from UC and target VM

5) Once all files were copied from both the investigative VM and target VM, they were both shut down, compressed into password protected .zip files using 7-zip and a hash value was calculated and documented for both .zip files (Images 7 and 8). The password used for both .zip files will be included in a separate document.

Image 7 Hash values of compressed investigative VM

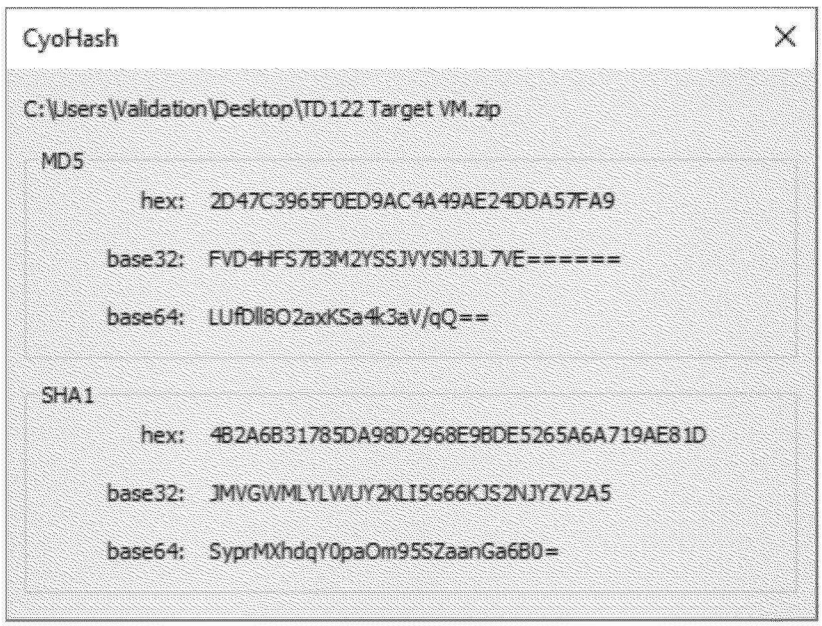

Image 8 Hash values of compressed target VM

F. ATTACHMENTS

i. The BitTorrent Protocol Specification – written by Brian Cohen
ii. Validation worksheet
iii. Validation stock photos folder
iv. Validation .torrent file

v. Wireshark captures
vi. Recording files for investigative VM
vii. Recording files for target VM
viii. Investigative VM
ix. Target VM

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

SUPPLEMENT TO
C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. hereby files this supplement pursuant to this court's oral order from October 3, 2019 at the Final Pre-Trial Conference regarding the testing and protocols discussed in the *U.S. v. Gonzalez*, 2:17-cr-001311-DGC.

There is no law enforcement privilege that precludes disclosure of material evidence.

The government argues that *Roviaro v. United States*, 353 U.S. 53 (1957), gives it a "privilege" not to disclose material evidence to Mr. Schwier. To the contrary, the *Roviaro* Court reversed the defendant's conviction, finding prejudicial error in the government's refusal not to disclose the name of its informer who "was the only witness in a position to amplify or contradict testimony of government witnesses." *Id.* at 64.

The U.S. Supreme Court and the Ninth Circuit have yet to recognize or reject a "law enforcement privilege." *Shah v. Dept. of Justice*,714 Fed. Appx. 657, 659 n.1 (9th Cir. 2017). No such privilege exists in *Roviaro*, which instead recognized a

limited "informer's privilege" that allows the government "to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law." 353 U.S. at 59.

Shah does not consider whether such a privilegewould comport with the sixth amendment rights of confrontation and compulsory process and the fifth amendment right to due process. Even in *United States v. Pirosko,* 787 F.3d 358 (6th Cir. 2015), where the defendant did not show materiality and the court upheld non-disclosure, the court cautioned that "this conclusion should not be read as giving the government a blank check to operate its file-sharing detection software sans scrutiny. As a general matter, it is important that the government's investigative methods be reliable, both for individual defendants like Pirosko and for the public at large." 787 F.3d at 366.

In *Roviaro,* the Supreme Court noted that:"[t]he scope of the privilege is limited by its underlying purpose." 353 U.S. at 60. Defense counsel does not intend to share the disclosed material with anybody other than his trial team, who often work under protective orders. Thus,there is no danger that child pornography distributors could find a way to avoid detection and thus render that tool of law enforcement ineffective, as the government claims. The government's argument presumes that somehow there will be wide disemintion of the software to the public. Mr. Fischbach is the firewall. He has previously been granted National Security clearance and no one has suggested he ever violated his oath to maintain those national security secrets. He has been subject to many non-disclsoure agreements and protective orders. No one has ever accused him of violating any. Balancing the government's concerns which do not rise to level of a recognized privilege with those of the defendant which are grounded in the fifth and sixth amendment, the so-called "law enforcement" privilege must give way.

The Court in *Roviaro* also ruled that "[a] further limitation on the applicability of the

privilege arises from the fundamental requirements of fairness. Where the disclosure of an informer's identity, or the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way." 353 U.S. at 60-61. "In these situations the trial court may require disclosure and, if the Government withholds the information, dismiss the action." *Id.* Thus, in *Roviaro,* the Court held that the privilege must give way. Because the informer, John Doe, was the person to whomRoviaro was accused of selling heroin,"his identity and testimony [were] highly material" and should have been disclosed. *Id.* at 62-63. The informer was "the sole participant, other than the accused, in the transaction charged" and "the only witness in a position to amplify or contradict the testimmony of government witnesses". Id. at 64.

The Torrential Downpour software and its associated materials plays the same role in this case that John Doe played in *Roviaro*. The program and its materials constitute "the only witness in a position to amplify or contradict the testimony" of SA Allison, the person who (according to the search warrant affidavit) downloaded child pornography from a remotely located computer on November 22, 2016. Not one scrap of contemporaneous evidence aside from date generated by Torrential Downpour software supports his claim.

This case is different from Gonzalez, and thus the test(s) that the defense wants to run are different.

The tests in Gonzalez as designed by the defense retained forensic examiner appeared aimed at answering specific questions pertinent to the facts of that case. In this case there are no .torrents on Mr. Schwier's alleged media that are relevant, and there is no data on the source computer or media that is relevant, unlike in the Gonzalez case. The Gonzalez defense identified nine tests it wanted to conduct in that case. See, *U.S. v. Gonzalez,* 2:17-cr-1311, at Doc. 86, Order of Court, August 27, 2019 at pg.3-4. And while these tests are of some interest, they do not address the specific issues identified in this case by the defense. As to the Gonzalez tests, tests 1 & 2 would not need to be run in this case if the government makes the same concessions it made

in Gonzalez. as described by the court. See, *U.S. v. Gonzalez*, 2:17-cr-1311, at Doc. 86, Order of Court, August 27, 2019 at pg. 8 lines 6-17 and pg.10 lines 6-10. The court also granted the defense request to conduct tests 3 & 4, and the parties agreed to tests 7, 8, & 9. The Gonzalez court noted that the main point of contention between the parties was whether the defense could have access to the ICAC COPS database. Id. at pg 3 line 19-21. The defense in this case does not need access to the ICAC COPS database.

The Gonzalez tests largely test the functionality of the software. The defense in this case wants to run a specific examination to test for a particular hypothesis, a particular condition that the defense believes it may have uncovered. And while the defense in this case does not need access to the ICAC COPS database, it does howeve r require that the government provide the .torrents that Torrentail Downpour Receptor identified as being files of interest and that were relied upon by SA Allison in conducting his Torrential Downpour searches in October and November of 2016.

To date no independent third party testing of Torrential Downpour has been done. And the testing done to date does not appear to meet basic scientific standards.

Mr. Schwier is not aware of any independent third party testing that has been done to date on Torrential Downpour. So far it appears that testing, to the limited extent that it exists, has been conducted by Detective Erdely. He is co-developer of the software and it appears he may have a financial interest and is a beneficairy of financial support provided by DOJ for the software. This appears to include as much as $4.4 million dollars in the last ten years in grants from the Department of Justice and does not include separate licensing fees received for the software. He has a clear bias and interest to show that the software works, and a clear interest in not releasing the program to anyone who wants to prove it may not work as intended. Indeed, testing by the software's co-developer engenders problems with confirmation bias. This is not how the scietific method works. Erdeley's hypothesis is that his software works as advertised. To test this hypothesis the scientific method requires testing the null hypothesis--- testing designed to prove

that the software does not work. If one is using the scientific method one does not design and run tests to show the software works rather you test for failure. Indeed, none of the reported testing appears to comply the the ISO/IEC/IEEE 29119 Software Testing-4: Testing Techniques. This standard is recognized by the National Institute of Standards and Technology (NIST) and by the Department of Justice. See also, National Institute of Standards and Technology, "Methodology Overview," published February 22, 2018 at [https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-general-0.]. The Erdely testing is designed to prove the functionality of the software, whereas the defense proposed testing will be designed to see it causes one particular or a set of particular circumstances.

The proposed defense test(s) is subject to attorney-client privilege and attorney work product doctrine. The defense will agree to disclose the particulars to the court in an ex parte proceeding only.

The circumstances to be tested by the defense team were identified by and during the defense forensic computer examination that has been on-going and largely conducted at the Orange County RCFL since May. It is also based upon information provided by Mr. Schwier to counsel. This examination has allowed Mr. Fischbach to identify specific data and files that are relevant to the proposed testing. Revealing the proposed test(s), and what data it is based upon would reveal attorney work product and attorney client privileged communications. Mr. Schwier will not disclose this information in court to the government, nor is he required to.

In other contexts, such as the issuance of Rule 17 subpoenas, the courts recognize that the defense need not disclose information that reveals attorney-client communications or work product or defense trial strategy. See, e.g., *United States v. McClure,* 2009 W.L. 937502 (E.D. Cal. 2009); *United States v. Crutchfield* (2014 W.L. 2569058 (N.D.Cal. 2014). The *McClure* and *Crutchfield* decisions both find that revealing defense trial strategy constitutes good cause for accepting the subpoena application *ex parte*. Local rules in other Districts

within the Ninth Circuit specifically authorize seeking a 17(c) subpoena *ex parte* for good cause and "good cause" is defined as, among other matters, avoiding the revelation of defense trial strategy. Even the trial court's protective order in *Budziak* (see attached) protected the testing and data generated by the defense tests from disclosure to the government.

In no other forensic field is the defense required to tell the government what independent tests it wants to run on any particular evidence. Whether the evidence is a controlled substance, or a hair, or DNA, so long as the evidence is material to the defense, the defense has a right to test and determine for itself what tests to run. If the results are not favorable the defense is not required to share that information with the government and need not use the results at trial. If the results are favorable the defense has the option of revealing the results and relying on those test results at trial. Of course, here the defense has no way to know in advance what the test results will show and whether the defense will intend to rely upon those results at trial. Mr. Schwier should not be required to disclose that information unless the defense intends to rely upon the evidence at trial. The test results could influence what type of defense Mr. Schwier intends to mount, and could affect his decision to proceed to trial or rather seek some sort of plea agreement. The data being relied upon and the test results are all matters that affect defense strategy, and thus pursuant to the fifth amendment and sixth amendment this information is privileged and not subject to disclosure.

Moreover, in no other defense testing of evidence is the defense required to conduct tests at a government facility. Here, the contraband evidence (actual images of child pornography) is subject to the restrictions imposed by the Adam Walsh act, and that evidence by statute must remain in government custody. The Torrential Downpour software is not contraband and not subject to those strictures. Moreover, the software is not classified as "Confidential Information" covered by the Confidential Information Procedures Act (CIPA) 18 U.S.C. App. 3 et seq. The defense has concerns whether the FBI offices can properly accommodate defense testing without the defense revealing privileged information, due to the

circumstances of the tests proceeding in a government facility. Moreover, Mr. Fischbach will require specific hardware and network configurations to conduct his tests and again the FBI may not be able to accommodate those needs. Mr. Fischbach's laboratory is already configured and set up to accommodate the testing contemplated.

Nevertheless, attached to Mr. Schwier's supplement brief, is a copy of the protective order issued by Judge Whyte in the *Budizak* case after the Ninth Circuit remand. This order fullly addresses the government's concern about protecting the software from *public* disclosure. Mr. Schweir respectfully suggests the court largely adopt the terms of this order, with notable exceptions, rather than the one utilized by the court in Gonzalez. Paragraph #3 is not applicable to this case and the defense sees no justifiable reason to conduct the testiing at a government facility. But the defense does agree with those terms of the *Budziak* Order holding that testing should not occur under the supervision or participation of the government, and that testing and results should remain confidential until the defense indicates that it intends to rely upon the tests and results at trial.

DATED at Anchorage, Alaska, this 15th day of October 2019.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
Phone 907-277-7171
Fax 907-277-0281
rmherz@gci.net
AK Bar No. 8706023

CERTIFICATE OF SERVICE
I hereby certify that on Oct 15, 2019, a copy of the foregoing Supp to C-3 Motion to Compel was served electronically on Assistant United States Attorney's Office s/ Robert Herz

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

ORDER REGARDING C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE

Before the Court at Docket 199 is Defendant Matthew William Schwier's C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software. The government responded in opposition at Docket 214 and filed supplemental briefing at Docket 219. Mr. Schwier filed supplemental briefing at Docket 221. An evidentiary hearing was held on October 17 and 18, 2019.

BACKGROUND AND PROCEDURAL HISTORY

On October 20, 2016, the Federal Bureau of Investigation ("FBI") used software called "Torrential Downpour" to purportedly identify Mr. Schwier's computer as possessing child pornography files that were available for download by third parties through BitTorrent, a peer-to-peer file-sharing network.[1] Torrential

[1] Docket 199 at 6; Docket 214 at 3. As described by Robert Erdely—offered by the government as an expert witness—a peer-to-peer network "allow[s] individuals unknown to each other and possibly separated by great distances to share files, such as audio and video files, freely." Docket 214-1 at 2, ¶ 7 (Decl. of Mr. Erdely).

Downpour is a piece of software developed for law enforcement personnel, to allow them to identify BitTorrent users who possess or seek to possess child pornography files.[2] The software operates similarly to other BitTorrent clients—like uTorrent, the program Mr. Schwier allegedly used[3]—with several important differences.[4] Unlike most BitTorrent clients, Torrential Downpour allows law enforcement to download files from a single user,[5] and does not itself share any files downloaded pursuant to an investigation.[6] On October 20, 2016, Torrential Downpour was unable to download the alleged child pornography available for distribution on Mr. Schwier's computer.[7]

In November 2016, the FBI again used Torrential Downpour to identify Mr. Schwier's computer as possessing child pornography that was available for download.[8] Over the course of three days, the FBI used Torrential Downpour to

[2] Docket 214-1 at 5, ¶ 16.

[3] Docket 214 at 3.

[4] Docket 214-1 at 5–6, ¶¶ 18–20.

[5] Docket 214-1 at 6, ¶ 19. "Traditionally, BitTorrent seeks to download from many sharing computers to speed up the download times." Docket 214-1 at 6, ¶ 19.

[6] Docket 214-1 at 6, ¶ 20.

[7] Docket 199 at 3–4; Docket 214 at 4.

[8] Docket 199 at 4–6; Docket 214 at 5.

download two files shared by Mr. Schwier's computer, one of which allegedly contained child pornography.[9]

In May 2017, the FBI seized multiple pieces of hardware from Mr. Schwier's home while executing a search warrant.[10] Forensic examination of the hardware identified multiple child pornography files, but could not find the particular files identified or downloaded by Torrential Downpour in October and November 2016.[11]

On August 16, 2017, the grand jury indicted Mr. Schwier on three counts of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).[12] A September 25, 2017 superseding indictment additionally charged Mr. Schwier with one count of distribution of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).[13] On April 24, 2019, the grand jury returned a Third Superseding Indictment that charged Mr. Schwier with two counts of possession of child pornography and one count of distribution of child pornography.[14]

---

[9] Docket 199 at 6; Docket 214 at 5.

[10] Docket 199 at 6; Docket 214 at 6.

[11] Docket 199 at 7; Docket 214 at 6.

[12] Docket 2.

[13] Docket 40 at 3 (Count 3).

[14] Docket 138. A Second Superseding Indictment had been filed on March 20, 2019. Docket 117.

The FBI's October 20, 2016 use of Torrential Downpour to identify child pornography files on Mr. Schwier's computer forms the basis of Count 1 in the Third Superseding Indictment.[15] The FBI's use of Torrential Downpour to download child pornography from Mr. Schwier's computer in November 2016 forms the basis of Count 2 in the Third Superseding Indictment.[16] Count 3 of the Third Superseding Indictment relates to the child pornography files found during the 2017 physical search of Mr. Schwier's hardware and is not related to the FBI's use of Torrential Downpour.[17]

Mr. Schwier retained Robert M. Herz, his current defense counsel, on March 12, 2018.[18] Mr. Herz retained Jeffrey M. Fischbach as an expert in computer forensics at least as early as November 2018.[19] Despite this, Mr. Herz did not file the instant motion to compel production of the Torrential Downpour software—the

[15] Docket 199 at 6; Docket 214 at 3–4.

[16] Docket 199 at 6; Docket 214 at 5.

[17] Docket 138 at 3.

[18] Docket 63.

[19] Docket 203-1 at 2, ¶ 4 (Decl. of Mr. Fischbach) (describing Mr. Fischbach's November 2018 request to review alleged child pornography file downloaded from Mr. Schwier's computer). And Mr. Schwier's supplemental briefing indicates that Mr. Fischbach had begun developing his thoughts about "[t]he circumstances to be tested" should he gain access to Torrential Downpour in May 2019. Docket 221 at 5.

foundation for two counts in the Third Superseding Indictment—until September 12, 2019, one month before trial was scheduled to begin.[20]

DISCUSSION

Mr. Schwier contends that Torrential Downpour "is flawed and should be tested and verified by a third party," and that the defense requires access to the program in order to effectively cross-examine government witnesses.[21] Mr. Schwier seeks disclosure of an installable copy of Torrential Downpour, along with its user and training manuals.[22] He does not seek disclosure of Torrential Downpour's source code.[23]

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E)(i), the government must disclose any "books, papers, documents, data . . . or copies or portions" thereof upon the defendant's request, provided that the item is in the government's control and is "material to preparing the defense."[24] "A defendant

---

[20] Docket 199; Docket 175 (setting trial date for October 15, 2019).

[21] Docket 199 at 9.

[22] Docket 199 at 9.

[23] Docket 199 at 9. However, Mr. Fischbach did request a copy of the Torrential Downpour source code during his testimony. Docket 229 at 3:2–18 (Excerpt of 10/17/2019 Evidentiary Hearing Tr.). The Court denies that request for the reasons discussed below.

[24] The defense also bases its motion on the Supreme Court's decision in *Brady v. Maryland*, 373 U.S. 83 (1963). The Court finds that case inapplicable and denies Mr. Schwier's motion to the extent it seeks disclosure of Torrential Downpour under *Brady*. *See United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *7 (D. Ariz. Feb. 19, 2019) (discussing applicability of *Brady* and finding that

must make a 'threshold showing of materiality' in order to compel discovery pursuant" to this rule.[25] "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense."[26]

In *Budziak*, the Ninth Circuit held that a district court had erroneously denied discovery of EP2P, a piece of investigative software similar to Torrential Downpour.[27] The Circuit concluded that the defendant had demonstrated materiality by "identif[ying] specific defenses to the distribution charge that discovery on the EP2P program could potentially help him develop."[28] The defense has done the same here; he presented evidence, through the declaration and testimony of Mr. Fischbach, suggesting that Torrential Downpour may have "exploit[ed] vulnerabilities in the [BitTorrent] protocols" to download files that Mr.

"[d]efendants have made no showing that Torrential Downpour will prove to be exculpatory or could be used to impeach a government witness").

[25] *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)).

[26] *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

[27] *Id.* at 1111–12.

[28] *Id.* at 1112.

Schwier had not made available for sharing.[29] Discovery of Torrential Downpour, then, could potentially help Mr. Schwier develop a defense to the distribution charge, as it is based solely on the FBI's use of the program to download files from Mr. Schwier's computer in November 2016.[30] Mr. Fischbach further explained, "it is critical to the defense . . . to understand how this software functions in order to determine its reliability and accuracy in identifying files reported as 'publicly available,'"[31] since Torrential Downpour's alleged October 20, 2016 identification of child pornography files on Mr. Schwier's computer is the sole basis for one of the possession charges.[32]

In light of this, the Court finds that Mr. Schwier has made the threshold showing of materiality required by Rule 16.[33] The Court further finds that the materiality of Torrential Downpour is limited to versions 1.15 and 1.23 of the

---

[29] Docket 200-1 at 7–8, ¶¶ 20–23; *see also Budziak*, 697 F.3d at 1112 ("[The defendant] submitted evidence suggesting that the FBI agents could have used EP2P software to override his sharing settings.").

[30] *See Budziak*, 697 F.3d at 1112 ("Given that the distribution charge . . . was premised on the FBI's use of the EP2P program to download files from [the defendant], it is logical to conclude that the functions of the program were relevant to his defense.").

[31] Docket 200-1 at 8, ¶ 24.

[32] Docket 200-1 at 9, ¶ 26; *see also Budziak*, 697 F.3d at 1112 (explaining that "[l]ike the competency of the drug-sniffing dog in [*United States v. Cedano-Areliano*, 332 F.3d 568, 571 (9th Cir. 2003)] the functions of the EP2P software constituted a 'very important issue' for Budziak's defense").

[33] *See Budziak*, 697 F.3d at 1112.

software—the versions used by the FBI during the events underlying the relevant counts in the Third Superseding Indictment.[34]

The government argues that even if the functionality, reliability, and accuracy of Torrential Downpour is material, disclosure of the software itself should be precluded by what it terms as a "law enforcement privilege."[35] In *Rovario v. United States*, the Supreme Court recognized the government's "privilege to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law."[36] The Supreme Court explained that "no fixed rule with respect to disclosure is justifiable" and directed courts to balance the public interest against the defendant's right to prepare his case, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors."[37] Courts have since applied this law enforcement privilege to investigative software like Torrential Downpour.[38]

---

[34] Docket 229 at 2:6–11.

[35] Docket 214 at 8–11.

[36] 353 U.S. 53, 59 (1957).

[37] *Roviaro v. United States*, 353 U.S. 53, 62 (1957).

[38] *See, e.g.*, *United States v. Pirosko*, 787 F.3d 358, 365–67 (6th Cir. 2015) (discussing the ShareazaLE software); *United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *8 (D. Ariz. Feb. 19, 2019) (discussing Torrential Downpour).

In *United States v. Gonzales*, the U.S. District Court for the District of Arizona recently applied the *Rovario* balancing test to Torrential Downpour, concluding that disclosure of an installable copy of the software to the defense was not warranted:

> Child pornography is a scourge, victimizing the most innocent for the basest of reasons. The government has a legitimate interest in preserving its ability to investigate and prosecute distribution of this material—distribution that creates the market and fuels the demand for creation of more child pornography. Agent Daniels testified that the government's investigative efforts would be severely hampered if a copy of Torrential Downpour got into the wrong hands. Countermeasures could be developed that would thwart law enforcement's monitoring of the BitTorrent network for suspected child pornography.[39]

The district court in *Gonzalez* did, however, allow the defense's expert to conduct certain testing of Torrential Downpour in a controlled setting at a secure government facility.[40]

The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that "child pornography distributors could find a way to avoid detection" if the workings of Torrential Downpour were made public, "render[ing]

---

[39] No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *8 (D. Ariz. Feb. 19, 2019).

[40] *Id.*; *see also United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 4040531, at *4–7, *10 (D. Ariz. Aug. 27, 2019) (specifying which tests the defense was permitted to run). The government's proposed validation protocol in this case tracks the August 2019 *Gonzalez* testing closely. *See* Docket 219 at 3 (comparing *Gonzalez* tests and government's proposed validation protocol); *see also* Docket 219-1 (government's proposed validation protocol).

that tool of law enforcement ineffective."[41] At the evidentiary hearing, Mr. Erdely testified that "to give [the defense] unfettered access to this software puts law enforcement and ten years of development at risk" because it would reveal certain aspects of Torrential Downpour's operation.[42]

Given the government's strong interest in retaining control of Torrential Downpour, the Court finds that disclosure of the software itself is not warranted, at least as of this juncture. The government has proposed to allow the defense to examine Torrential Downpour's operation while it is run by a government expert in a controlled environment.[43] Mr. Erdely testified that this validation process, which includes packet capture by a program called "Wireshark," would address the defense's questions about Torrential Downpour's functionality, accuracy, and ability to exploit vulnerabilities in the BitTorrent protocol.[44]

The Court acknowledges Mr. Schwier's interest in understanding the operation of Torrential Downpour as it relates to his defense, and the Court concludes based on the present record that the validation process proposed by

---

[41] Docket 214-1 at 7, ¶ 23.

[42] Docket 230 at 8:25–9:2 (Excerpt of 10/18/2019 Evidentiary Hearing Tr.). *But see* Docket 221 at 2–3 (defense argument that Mr. Fischbach is trustworthy and is "a firewall" that will prevent Torrential Downpour's dissemination to the public).

[43] *See* Docket 219-1 (proposed validation process).

[44] Docket 230 at 9–17; *see also* Docket 230 at 10:24–11:5 ("[I]f there was a vulnerability and our software was designed to exploit these vulnerabilities, . . . it would be exposed in the Wireshark packet capture.").

the government is sufficient to meet the defense's needs. Mr. Fischbach had multiple opportunities to identify specific deficiencies in the government's proposed validation protocol, but was not able to do so in a way that persuaded the Court that additional or more extensive testing was necessary.[45] Mr. Fischbach testified that the proposed testing would not show how two features of Torrential Downpour—single-source downloading and the inability to upload—affect the BitTorrent protocol, if at all.[46] But when asked about the materiality of this information, Mr. Fischbach was only able to speak in vague generalities, claiming attorney-client privilege.[47] And while the defense contends that it has begun to formulate tests for Torrential Downpour that may be helpful to the defense, it has not identified these tests or explained how they differ from the government's

[45] Docket 230 at 2–8 (Mr. Fischbach discussing the government's proposal). Mr. Fischbach, in his first declaration, expressed a concern that Torrential Downpour was exploiting vulnerabilities in either BitTorrent itself or in BitTorrent clients, such as uTorrent. Docket 200-1 at 7, ¶¶ 20–21. But Mr. Erdely persuasively testified that the specific uTorrent exploit identified by Mr. Fischbach had been resolved in 2014, well before the events of this case. Docket 214-1 at 12, ¶ 33. Moreover, as explained above, Mr. Erdely also persuasively testified that the use of packet capture, as specified in the government's proposed validation protocol, would reveal whether Torrential Downpour exploited any vulnerabilities. Docket 230 at 10:24–11:5.

[46] Docket 230 at 3:20–4:2, 6:3–16.

[47] Docket 230 at 6:24–7:4 ("[T]he findings that we have, and, again, I'm being careful as far as privilege goes, the findings that we have have demonstrated some oddities possibly, but, again, they have to be tested to see if they are associated, but they certainly cause concern.").

proposed validation protocol, claiming that the defense's proposed testing ideas are confidential attorney work product and subject to the attorney-client privilege.[48]

The Court cannot rule on the materiality of forensic tests that have not been disclosed to it. But the Court will accord the defense one last opportunity to explain what additional testing it is seeking and why. Accordingly, within **seven days of this order**, the defense may file a supplemental declaration of its expert that: (1) explains the specific hypotheses the defense seeks to test; (2) describes with particularity the test(s) the defense seeks to conduct; and (3) identifies the specific hardware and configurations necessary to complete that testing. The declaration shall also clearly explain why the government's proposed validation testing would not be adequate. This declaration may be filed ex parte or redacted, but only to the extent necessary to protect confidential attorney work product and/or privileged attorney-client communications.

CONCLUSION

In light of the foregoing, the motion at Docket 199 is GRANTED IN PART and DENIED IN PART.

IT IS HEREBY ORDERED that the validation process described at Docket 219-1 shall be carried out for versions 1.15 and 1.23 of the Torrential Downpour

[48] Docket 221 at 5–6; *see also* Docket 221 at 4 ("The defense in this case wants to run a specific examination to test for a particular hypothesis, a particular condition that the defense believes it may have uncovered.").

software on November 4, 2019, and on November 5, 2019 as necessary. The validation shall take place in a secure setting at a government location in Anchorage, Alaska that is selected by the government. Defense counsel and Mr. Fischbach may be present and may observe the validation process.

As discussed on the record,[49] the Court further enters a protective order with regard to the validation process as follows:

1. Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person without prior order of the Court.
2. Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this

[49] Docket 230 at 8:14–20.

case, provided the materials are filed under seal and/or submitted to the Court for *in camera* inspection.

3. Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

In the event a timely supplemental expert declaration is filed by the defense, the Court may amend this order as warranted after the government has had an opportunity to respond.

DATED this 24th day of October, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

SUPPLEMENTAL ORDER REGARDING C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE

On October 24, 2019, after an evidentiary hearing, the Court entered an order at Docket 231 that granted in part and denied in part Defendant Matthew William Schwier's C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software at Docket 199. The Court directed the government to conduct certain validation testing of the Torrential Downpour software in the presence of the defense.[1] The October 24, 2019 order set out the factual background relevant to this issue and it is not repeated here.[2]

The Court's October 24, 2019 order allowed the defense to file a supplemental declaration of its expert to explain why it believed additional testing was necessary, and the Court notified the parties that it may amend its order as

[1] Docket 231 at 12–14.

[2] *See* Docket 231 at 1–12.

warranted in light of that declaration.[3] On October 31, 2019, the defense timely filed a supplemental ex parte declaration of Jeffrey M. Fischbach, offered as a computer forensics expert.[4] The defense filed a redacted copy of Mr. Fischbach's declaration on the same day, from which it had removed all information it claimed as privileged.[5]

On November 1, 2019, the government filed a motion responding to Mr. Fischbach's redacted declaration, asking the Court to either hold an immediate status hearing or issue an order finding that the defense had not shown that additional tests were material.[6]

The Court granted the government's motion and held a brief status conference on November 4, 2019,[7] after which the parties conducted validation testing of the Torrential Downpour software pursuant to the Court's October 24, 2019 order.[8] The Court held a second status conference after the completion of the validation process, on November 5, 2019, at which it notified the parties that it

[3] Docket 231 at 12, 14.

[4] Docket 233.

[5] Docket 234.

[6] Docket 235.

[7] Docket 240.

[8] *See* Docket 231 at 12–13 (ordering government to conduct "the validation process described at Docket 219-1").

would issue a written order that would address whether additional testing would be ordered in light of Mr. Fischbach's October 31, 2019 declaration.

DISCUSSION

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E)(i), the government must disclose any "books, papers, documents, data . . . or copies or portions" thereof upon the defendant's request, provided that the item is in the government's control and is "material to preparing the defense." "A defendant must make a 'threshold showing of materiality' in order to compel discovery pursuant" to this rule.[9] "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense."[10]

In *United States v. Budziak*, the Ninth Circuit held that a district court had erroneously denied the defense's request for discovery of EP2P, a piece of investigative software similar to Torrential Downpour.[11] The Circuit concluded that the defendant had demonstrated materiality by "identif[ying] specific defenses to

[9] *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)).

[10] *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

[11] *Id.* at 1111–12.

the distribution charge that discovery on the EP2P program could potentially help him develop."[12] The Circuit cautioned:

> In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless[,] . . . especially . . . where . . . a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software.[13]

It explained that "[a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately."[14] In its October 24, 2019 order, the Court found that the functionality, reliability, and accuracy of Torrential Downpour were material to Mr. Schwier's defense.[15]

However, the government asserted that production of the software was precluded by the law enforcement privilege recognized in *Roviaro v. United* States,

---

[12] *Id.* at 1112. The defendant in *Budziak* "presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his 'incomplete' folder, making it 'more likely' that he did not knowingly distribute any complete child pornography files to [federal] [a]gents." *Id.* He also "submitted evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings." *Id.*

[13] *Id.* at 1112–13.

[14] *Id.* at 12 (quoting *United States v. Leibert*, 519 F.2d 542, 547–48 (3rd Cir. 1975).

[15] Docket 231 at 7–8.

353 U.S. 53 (1957).[16] Balancing the government's interest against the defendant's,[17] the Court found in its October 24, 2019 order that based on the record then before it, "the validation process proposed by the government [was] sufficient to meet the defense's needs."[18] The Court noted that Mr. Fischbach had spoken only in generalities at the evidentiary hearing about why production of the software for additional testing by him was necessary to the defense.[19] Mr. Fischbach claimed that the defense's proposed testing ideas were confidential attorney work product and subject to the attorney-client privilege.[20] The Court concluded that it could not "rule on the materiality of forensic tests that have not been disclosed to it."[21]

In the ex parte portion of his subsequent October 31, 2019 declaration, Mr. Fischbach described four additional tests of the Torrential Downpour software that

---

[16] Docket 214 at 8–11.

[17] *See Roviaro*, 353 U.S. at 62 (directing courts to balance public interest in protecting flow of information to government against defendant's right to prepare his case, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors").

[18] Docket 231 at 10–11.

[19] Docket 231 at 11.

[20] *See, e.g.*, Docket 230 at 6:24–7:4 (Excerpt of October 18, 2019 Hearing Transcript) ("[T]he findings that we have, and again, I'm being careful as far as privilege goes, the findings that we have have demonstrated some oddities possibly, but, again, they have to be tested to see if they are associated, but they certainly cause concern.").

[21] Docket 231 at 12.

he seeks to conduct at the Regional Computer Forensics Lab ("RCFL") in Anaheim, California.[22] Mr. Fischbach explained that these four tests are necessary to either develop or rule out specific defense strategies related to Counts 1 and 2 of the Third Superseding Indictment, both of which are premised on the FBI's use of the Torrential Downpour software.[23]

In the redacted copy of Mr. Fischbach's declaration, the entire description of these four tests and their relevance to the defense are blacked out.[24] The government argues that "[b]y redacting the tests themselves, the defense has withheld from the government any opportunity to contest the tests, or to agree with them."[25] The Court acknowledges the government's concerns and recognizes that in *United States v. Gonzales*, the defense disclosed the actual tests it wanted to run on Torrential Downpour in a way that permitted the government to argue against the testing.[26] Nevertheless, the Court is prepared to balance the defense's need for the additional testing of Torrential Downpour against the government's interest in restricting further access to the software.

---

[22] Docket 233-1 at 7–10, ¶ 23; Docket 234-1 at 7–10, ¶ 23 (redacted).

[23] Docket 233-1 at 7–10, 11 ¶¶ 23, 28; Docket 234-1 at 7–10, 11 ¶¶ 23, 28 (redacted); *see also* Docket 231 at 4 (describing basis of counts in indictment).

[24] Docket 234-1 at 7–10, ¶¶ 23, 28.

[25] Docket 235 at 3.

[26] No. CR-17-01311-001-PHX-DGC, 2019 WL 4040531, at *4–7 (D. Ariz. Aug. 27, 2019) (describing six tests and government's objections to their materiality).

Upon review of Mr. Fischbach's October 31, 2019 declaration, the Court concludes that requiring the Torrential Downpour software to be accessible to Mr. Fischbach for the additional testing at the Anaheim RCFL is warranted. In reaching this conclusion, the Court has considered that the government's interest in prosecuting Mr. Schwier for child pornography is not eviscerated by ordering the software's production. The government may opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense. In that event, the government may still proceed on Count 3.[27] The Court also notes that the government would have the opportunity to assert that the conduct alleged in Counts 1 and 2 constitutes relevant conduct for sentencing purposes in the event Mr. Schwier is adjudged guilty on Count 3.

CONCLUSION

In light of the foregoing, the Court supplements its order at Docket 231 as follows:

(1) **Within seven days of the date of this order**, the government shall make the Torrential Downpour software available to Mr. Fischbach and defense counsel at the Regional Computer Forensics Lab in Anaheim, California, for a

[27] *United States v. Gonzales*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *8 (D. Ariz. Feb. 19, 2019) ("When the two interests come squarely into conflict, the defendant's right to a fair trial should prevail because the government can always choose to protect its investigative technique by dropping the prosecution and due process dictates that a citizen should never be convicted in an unfair trial." (citing *United States v. Turi*, 143 F. Supp. 3d 916, 921 (D. Ariz. 2015))).

period of 21 consecutive days for additional testing. This testing shall be limited to the four tests described in Mr. Fischbach's October 31, 2019 declaration.

(2) The government may propose additional terms to the protective order entered at Docket 231 as warranted.

DATED this 8th day of November, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

BRYAN SCHRODER
United States Attorney

JONAS M. WALKER
CHARISSE ARCE
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: jonas.walker@usdoj.gov
charisse.arce@usdoj.gov
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER AND NOTICE OF COMPLIANCE WITH SUPPLEMENTAL ORDER (Dkt. 243)

The United States, through undersigned Assistant U.S. Attorney, responds to the Supplemental Order Regarding C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour (the "Order," Dkt. 243). As explained below, the government has been working diligently to meet the Order's one-week deadline, and the computer can be available on November 20, 2019.

A) The government elects to provide limited access to a computer running Torrential Downpour, rather than dismiss Counts 1 and 2.

The Order permits the government to choose between only two options: first, allowing the defense to perform four tests on Torrential Downpour, the nature of which are withheld from the government; or, second, dismissing Counts 1 and 2.[1] The Order is silent regarding technical aspects of how the government must provide the computer.

In the event the Court orders the additional terms of the protective order, below, the government is electing to provide access consistent with the Order, rather than dismissing Counts 1 and 2. The government is selecting this option because the Order does not compel internet access for the computer; nor does it permit the defense to add or remove software or hardware from the computer; nor does it allow the computer to leave the Orange County Regional Computer Forensics Lab (OCRCFL).[2] Most importantly, and consistently with the Court's prior protective order at Dkt. 231, the Order does not result in the software itself being released into "the wild." Finally, the Order leaves in place the broad protective language in Dkt. 231.[3] Thus, the order strikes a "proper balance" between production and

[1] "The government may opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense. In that event, the government may still proceed on Count 3." Order, Dkt. 243, at 7.

[2] The OCRCFL is located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. *See* Order Re: Compliance With Discovery Procedure, Dkt. 158 at footnote 4 regarding referring to the OCRFCL as the "Anaheim RCFL."

[3] The Court ordered:

> Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other

protection Roviaro v. United States, 353 U.S. 53 (1957).

Accordingly, the government is preparing a computer for defense access at the OCRCFL. The government will take reasonable measures to ensure that the computer will not access the internet, for several reasons. First, the Court did not order internet access. *See* Order, Dkt. 243. Second, because Torrential Downpour is designed to, and does reliably, download child pornography, connecting it to the internet would create a risk that it would fulfill its intended function, thereby facilitating the distribution of child pornography, in violation of 18 U.S.C. § 2252A, and other applicable laws, which the Order does not permit. Third, the Court did not order the defense to have access to ICAC COPS, which could be accessible via the internet. Likewise, the government will take reasonable measures to ensure that Torrential Downpour cannot be digitally or physically removed from the computer.

B) Additional terms for a protective order

Pursuant to paragraph (2) of the Order at Dkt. 243 at 7, the government respectfully requests the Court order the following additional terms to a protective Order:

1. The government will provide a computer at the OCRCFL. The computer will have one version of Torrential Downpour installed, *i.e.*

---

than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person without prior order of the Court.

Dkt. 231 at 13.

version 1.23, one of the versions used in this investigation. The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

2. The only persons who will have access to the computer are Jeffrey Fischbach and Robert Herz (collectively "the defense"). The defense will have access to the computer for 21 consecutive days of testing.

3. The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.

4. The defense may bring digital media, computers, and phones into the room with the computer.

5. The defense will not remove the computer from the OCRCFL. The defense will not copy Torrential Downpour.

6. The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape.

7. The defense will not download or distribute child pornography using the computer. Any downloading of child pornography would constitute a violation of the federal criminal code.

8. All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain the Wireshark data pending further order of the Court.

9. At the conclusion of testing, the FBI will "zip" all the Wireshark files, meaning it will use software to compress them. The FBI will "hash" the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government believes that these restrictions should permit the defense to perform any legitimate testing on Torrential Downpour, while, also, ensuring that the software is not removed from the computer.

The Court is familiar with Wireshark; it is the screen-recording and packet-capturing program the government used during the validation testing previously ordered

by the Court.[4] For the current testing, the preservation of Wireshark data accomplishes two goals. First, it creates some measure of protection against the copying of Torrential Downpour. Second, it protects the integrity of the testing process. To the extent that Mr. Fischbach testifies pursuant to FRE 702, the Wireshark data would be the best possible evidence regarding the testing.

C) Objections to defense's *ex parte* advocacy.

In an abundance of caution, and to preserve the record, the government notes that, on record on November 4 and 5, 2019, prior to the Court issuing the Order, the government objected to the Court's consideration of the defense's *ex parte* communication. *See* Dkt 234-1 (redacted version of Mr. Fischbach's declaration). The government respectfully maintains its objections to the Court's consideration of the defense's *ex parte* communications.

On October 17 and 18, 2019, the parties' expert witnesses testified at length. Following that hearing, the Court ordered the government's proposed testing and denied the defense's request that the government produce Torrential Downpour. Dkt. 231. This order made sense in light of the defense's failure to identify the tests and Mr. Fischbach's performance under cross-examination.[5]

Having failed to meet its burden under Budziak at the evidentiary hearing, the defense later submitted, *ex parte*, a Declaration of Jeffrey M. Fischbach, dated October 31,

[4] *See* Dkt. 219-1 at para. 3; Dkt. 231 at 12.
[5] "But when asked about the materiality of this information, Mr. Fischbach was only able to speak in vague generalities, claiming attorney-client privilege." Dkt. 231 at 11.

2019, a redacted version of which the government received at Dkt. 234-1. As the Court notes in the Order, "[i]n the redacted copy of Mr. Fischbach's declaration, the entire description of these four tests and their relevance to the defense are blacked out." Order at 243 at 6. Thus, it was not until October 31 that the defense identified the tests, long after the government's opportunity to challenge the merits of Mr. Fischbach's claims had passed. In this way, the defense achieved, via *ex parte* advocacy, that which it failed to do when Mr. Fischbach was subject to cross-examination in open court.

"[I]n our system, adversary procedures are the general rule and *ex parte* examinations are disfavored." United States v. Kenney, 911 F.2d 315, 321 (9th Cir. 1990). The "reliability [of evidence is] assessed in a particular manner: by testing in the crucible of cross-examination." Crawford v. Washington, 541 U.S. 36, 61 (2004). "This open examination of witnesses is much more conducive to the clearing up of truth" because "adversarial testing beats and bolts out the Truth much better." Id. (internal citations and punctuation omitted). The Supreme Court has described cross-examination as the "greatest legal engine ever invented for the discovery of truth." Maryland v. Craig, 497 U.S. 836, 846 (1990).

Due to the *ex parte* nature of the defense's advocacy, the government is ignorant of the four tests, their procedures, goals, scientific validity, and technological requirements. Accordingly, the government has had no opportunity to contest their materiality under United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012). As the Court has already

acknowledged[6], the government has a legitimate interest in protecting Torrential Downpour, pursuant to Roviaro v. United States, 353 U.S. 53 (1957). The government's interest in protecting, and responsibility to protect, this important tool for investigating child pornography is especially heightened when, as here, the government has been kept ignorant of the tests that the defense is requesting.

Moreover, the secrecy of the tests has complicated the government's response to the Order. Due to the nationwide importance of protecting Torrential Downpour, while also effectively prosecuting child pornography offenses, the decision regarding how to respond to the Order is not solely that of the U.S. Attorney's Office for the District of Alaska. Accordingly, in the four working days since the Court issued the Order, the government has conferred with the FBI Office of General Counsel; the Child Exploitation and Obscenity Section of the Criminal Division of the U.S. Department of Justice; another U.S. Attorney's Office; in addition to personnel involved in this investigation.

//

---

[6] The Court held:

> The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that "child pornography distributors could find a way to avoid detection" if the workings of Torrential Downpour were made public, "render[ing] that tool of law enforcement ineffective." At the evidentiary hearing, Mr. Erdely testified that "to give [the defense] unfettered access to this software puts law enforcement and ten years of development at risk" because it would reveal certain aspects of Torrential Downpour's operation.

Order Regarding C-3 Motion, Dkt. 231 at 10-11.

D) Conclusion: The computer will be available by November 20, 2019.

The FBI has advised the undersigned that it can have the computer prepared and in place at the OCRCFL, ready for the defense, by Wednesday, November 20, 2019. The government respectfully requests the Court issue the attached protective order, the terms of which are essential to protect Torrential Downpour, and which should not interfere with any testing by the defense. Absent these protections, the government cannot provide the computer.

The government objects to any additional *ex parte* advocacy by the defense, particularly regarding the terms of the protective order. If necessary, the government can provide an affidavit, or the testimony of a witness, to explain the merits of the terms of the protective order.

RESPECTFULLY SUBMITTED November 15, 2019, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Jonas M. Walker
JONAS M. WALKER
Assistant U.S. Attorney
United States of America

CERTIFICATE OF SERVICE

I hereby certify that on November 15, 2019,
a true and correct copy of the foregoing
was served electronically on the following:

Robert M. Herz

s/ Jonas M. Walker
Office of the U.S. Attorney

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

[PROPOSED] ORDER GRANTING MOTION FOR ADDITIONAL TERMS FOR ROTECTIVE ORDER

Having duly considered the United States' Motion for Additional Terms for Protective Order and Notice of Compliance with Supplemental Order (the "Motion"), the Court grants the Motion and ORDERS that:

1. The government will provide a computer at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The computer will have one version of Torrential Downpour installed, *i.e.* version 1.23, one of the versions used in this investigation. The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

//

2. The only persons who will have access to the computer are Jeffrey Fischbach and Robert Herz (collectively "the defense"). The defense will have access to the computer for 21 consecutive days of testing.

3. The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.

4. The defense may bring digital media, computers, and phones into the room with the computer.

5. The defense will not remove the computer from the OCRCFL. The defense will not copy Torrential Downpour.

6. The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape.

7. The defense will not download or distribute child pornography using the computer. Any downloading of child pornography would constitute a violation of the federal criminal code.

8. All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain

the Wireshark data pending further order of the Court.

9. At the conclusion of testing, the FBI will "zip" all the Wireshark files, meaning it will use software to compress them. The FBI will "hash" the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government may provide the computer by November 20, 2019. The government's compliance with this Order satisfies the government's obligations under United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).

Moreover, the Court reaffirms its prior protective Order (Dkt. 231), as follows:

Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person

without prior order of the Court.

Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this case, provided the materials are filed under seal and/or submitted to the Court for in camera inspection.

Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

DATED this _____ day of November, 2019, at Anchorage, Alaska.

_____
UNITED STATES DISTRICT COURT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

ORDER FOR GOVERNMENT TO REPLY TO DEFENSE'S RESPONSE IN OPPOSITION AT DOCKET 248 AND COMPELLING PRODUCTION OF VALIDATION TESTING RECORDS

Before the Court at Docket 244 is the government's motion proposing additional terms for the protective order governing production of the Torrential Downpour software.[1] Pursuant to the Court's order at Docket 247, the defense has responded in opposition and filed a redlined copy of the government's proposed order.[2] The defense disputes several elements of the government's proposed protective order, including a term that would prohibit internet access during testing.[3] Having reviewed the defense's opposition, the Court directs the

[1] *See* Docket 231 at 13–14 (entering protective order); *see also* Docket 243 at 8 (allowing government to "propose additional terms to the protective order entered at 231 as warranted").

[2] Docket 248; *see also* Docket 249 (Decl. of Jeffrey Fischbach in support of Response in Opposition).

[3] Docket 248 at 2–3; *see also* Docket 249 at 5, ¶ 19 ("[I]n order to complete *any* of my proposed tests, and as a requirement of the software itself, I *must* have internet access." (emphasis in original)); Docket 244 at 4 (proposing that software be tested on computer without access to the internet).

government to file a brief reply, giving special attention to the question of internet access.[4]

The defense's response in opposition also claims that the government has not yet produced the results of the November 4, 2019 validation testing of the Torrential Downpour software.[5] At the November 5, 2019 status conference, the government stated that it believed it could "overnight [the validation data] on Thursday, have it down to the Orange RCFL on Friday, the 8th [of November]."[6] According to the defense, Detective Erdely also indicated that he planned to prepare a report on the validation testing.[7] The Court hereby orders the government to produce to the defense the validation data and Detective Erdely's report immediately or, failing that, to explain why doing so is impossible in its reply.

Accordingly, IT IS ORDERED that the government shall file a reply to the defense's opposition no later than **November 20, 2019 at 5:00 p.m.** IT IS FURTHER ORDERED that the government shall produce the data from the November 5, 2019 Torrential Downpour validation and the accompanying report

---

[4] *See* L. Crim. R. 47.1(c) ("Unless otherwise ordered by the Court, no reply memorandum will be filed.").

[5] Docket 248 at 4.

[6] Docket 250 at 2:17–22 (Partial Tr. of Nov. 5, 2019 Status Conf.).

[7] Docket 250 at 5–8 (Defense counsel's stating that "Detective Erdely indicated that the earliest he thought he could have a package of data available for release, he wanted time to write a report, the earliest that could be ready would be Friday [November 8, 2019].").

to the Orange RCFL for review by the defense as soon as possible upon receipt of this order. If such production is impossible, the government shall provide an explanation in its reply.

DATED this 19th day of November, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

BRYAN SCHRODER
United States Attorney

JONAS M. WALKER
CHARISSE ARCE
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: jonas.walker@usdoj.gov
charisse.arce@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

MOTION FOR PARTIAL RECONSIDERATION REGARDING ORDER (Dkt. 254) AND FOR TELEPHONIC PARTICIPATION OF WITNESS AT STATUS HEARING

The United States, by undersigned Assistant United States Attorney, pursuant to L.Civ.R. 7(h)(1)(A), respectfully moves the Court for partial reconsideration of the Order Re Motion for Additional Terms for Protective Order (Dkt. 244) (the "Order," Dkt. 254), and pursuant to L.Civ.R. 7(i), telephonic participation by a witness. The government

respectfully requests an opportunity to present the testimony of a witness to explain the issues discussed below.

In the 14 days since the Court originally ordered the government to make Torrential Downpour available to the defense (Dkt. 243), the government has diligently worked to craft an appropriate protective order that complies with both United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012), and Roviaro v. United States, 353 U.S. 53 (1957). In an unprecedented development, the United States has agreed to allow a defense expert to test Torrential Downpour outside the presence of a government agent. The government has, in good faith, rapidly proposed two protective orders. Taking into account the defense's objections to the first proposed order (244-1), the government crafted a second proposed protective order (253-4) that allowed internet access, but required Wireshark as a way to protect the software from copying.

A) Wireshark provides some assurance against software copying, but imposes no costs on the defense.

The Court held (Order at 2) that FRCrP 16 does not impose a duty on the defense to preserve evidence. The government does not dispute this legal conclusion.

However, the Order overlooked, and did not address, an important reason the government seeks a protective order with Wireshark or another appropriate packet-capture software: *i.e.* detecting digital copying of Torrential Downpour from the TD Computer.

Put another way: there are two potential ways that Torrential Downpour could be compromised at the OCRCFL; first, being physically removed from the OCRCFL; or, second, which is more likely to occur, being digitally copied from the TD Computer onto

other media. The Court has adequately protected Torrential Downpour from being physically removed from the OCRCFL by ordering that the defense will not open, tamper with, or remove the TD Computer from the OCRCFL.

However, the Order provides no way to verify that Torrential Downpour has not been copied from the TD Computer. The risk is that, during testing, the defense could inadvertently copy Torrential Downpour onto the digital media or computers that will be brought into the room with the TD computer. Copying Torrential Downpour would be as easy as copying any file. To be clear, the government is not accusing the defense of intending violate a protective order, or conspiring to violate 18 U.S.C. § 1030, or otherwise attempting to copy the software from the TD Computer. Rather, the government is seeking a reasonable prophylactic measure that will confirm that the software has not been copied.

Mr. Fischbach has, already, lost a hard drive at the OCRCFL in this case. *See* Dkt. 253-2 (email from Joe Monroe, stating "Fischbach advised he was missing an external hard drive that he left in the Defense Review room, during his last visit. We were unable to locate the missing external hard drive").[1] Given the high importance of protecting Torrential Downpour from disclosure, such negligence is reasonable cause for concern, particularly in light of the government's evidence that Torrential Downpour must be protected from disclosure.

> The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that "child pornography distributors could find a way to avoid detection" if the workings of Torrential Downpour were made

1 The government's understanding is that Mr. Fischbach insinuated that the OCRCFL was at fault.

> public, rendering that tool of law enforcement ineffective. At the evidentiary hearing, Mr. Erdely testified that to give the defense unfettered access to this software puts law enforcement and ten years of development at risk because it would reveal certain aspects of Torrential Downpour's operation.

Dkt. 231 at 9-10 (internal punctuation omitted).

Moreover, given his purported experience with classified information, Mr. Fischbach should be comfortable complying with procedures intended to verify that sensitive information is not inadvertently lost during discovery. Indeed, that is the very purpose of the OCRCFL.

Finally, Wireshark provides significant protections for the government, but imposes no costs on the defense. Wireshark will not interfere with any privileged information, because the government will not possess the Wireshark data. Wireshark will not interfere with any testing the defense runs.

The government respectfully requests a status hearing with an opportunity to present the telephonic testimony of a witness who can explain the security value of Wireshark.

B) The government is working to comply with other aspects of the Order (Dkt. 254).

The government has identified a computer with specifications similar to the one already in use in this case. Per Mr. Herz's email at Dkt. 253-3, such a computer should satisfy the defense.

The Court ordered the government to "provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements" by the end of one working day. Order at 254. The Court did not define "all applicable TD software documentation." The government is diligently

working to identify a manual for those two versions of Torrential Downpour and redact the privileged information therefrom for discovery.

C) Conclusion

The government respectfully requests the Court schedule a status hearing on November 25 or 26, 2019, at which the government may present the testimony of a witness to briefly explain why Wireshark (or another packet capture program) is important to protect Torrential Downpour from being compromised during testing. In the event that the Court rejects the use of any packet-capture software, the government may request an additional period to propose an alternative technical arrangement that would permit the defense to do testing.

RESPECTFULLY SUBMITTED November 22, 2019, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Jonas M. Walker
JONAS M. WALKER
Assistant U.S. Attorney
United States of America

CERTIFICATE OF SERVICE

I hereby certify that on November 22, 2019,
a true and correct copy of the foregoing
was served by served through ECF on:

Robert Herz

s/ Jonas M. Walker
Office of the U.S. Attorney

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

MOTION FOR PARTIAL RECONSIDERATION OF THE COURT'S ORDER AT DOC.254 RE: ADDITIONAL TERMS FOR PROTECTIVE ORDER

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. pursuant to L.Civ.R. 7.3(h)(1)(A), and the fifth and six amendments of the United States Constitution, hereby moves this court for partial reconsideration of its Order at Doc.254 due to a "manifest error of fact."

On November 8, 2019 the court ordered the government at Doc. 243 to provide the defense with a copy of the government's secret proprietary software "Torrential Downpour" used by the government in its surreptitious investigation of Mr. Schwier in this case, so that it could be subjected to independent third party testing, to test among other things the reliability and accuracy of the software. The court gave the government 7 days to comply with the order. The court also invited the government to propose additional terms to the protective order previously entered at Doc.231 if "warranted." On the day the government was ordered to release the software, the government at Doc.244 filed a motion seeking to add terms to the protective order previously issued at Doc.231. Following additional briefing by the parties, the court issued the Order at Doc.

254 which added additional terms to the protective order at Doc. 231, and from which the defense now seeks partial reconsideration.

The most significant manifest error of fact in the court's order is paragraph 9 which limits the defense to the use of one port and network connection. Factually this error, as explained by Mr. Fischbach in his Declaration in Support of this motion filed herewith, will make it impossible for him to conduct any of the proposed defense tests which this court has deemed material to defense preparation for trial. See, Fischbach Declaration in Support of Defense Motion for Partial Reconsideration of Court's Order at Doc. 254 [hereinafter "Fischbach Declaration]. See, e.g. paragraph 2 and 5e.

As Mr. Fischbach notes: this restriction prevents him from installing industry accepted software and hardware as well as prevents him from removing his test results from the government provided computer for further examination and analysis on his own equipment, and/or in his own forensic work environment. He would be unable to connect a screen, keyboard, or mouse, let alone the hardware and software that he needs for his tests. The hardware and software required and vetted by industry standard forensic practice would insure more than any prophylactic proposed by the government that no data accidentally alter results or escape the system. Specifically, he writes:

> I simply *must* have the ability to connect my own equipment, install my own industry-tested and accepted software and hardware, and to have the ability to remove my results for further examination and analysis. Otherwise, I *cannot* complete the testing that has been found material in this matter. *In short, I need access to multiple computer ports and network connections to run my tests.*

See, Fischbach Declaration at paragraph 5(e) emphasis supplied. This factual error in the court's order must be corrected in order for defense testing to be accomplished.

The manifest error of fact in Paragraphs 6 and 7 of the court's order is that these additional terms compromise attorney-client privilege and attorney work product by intruding

upon the confidential and independent defense testing process. These restrictions do not actually provide security to prevent the loss of TD software "into the wild," but they do prevent the defense from conducting its tests properly and from implementing time-tested forensic-standard procedures (software and hardware) for securing sensitive data. See, Fischbach Declaration at 5(a)-(c). Moreover, requiring the government to be the sole possessor of the password protecting the TD test equipment, both inserts the government into the defense chain of custody and also makes it impossible for Mr. Fischbach to be held accountable for securing either the TD software or his own results as the government now has access to defense work product. Indeed, the only person who should have sole access to defense work product is Mr. Fischbach, and as such he should have sole and exclusive possession of any passwords. Mr. Fischbach sets out the problems presented by these restrictions in detail in his declaration but a few highlights appear below.

While having the government start the computer each time and enter a password seems innocuous, it is not. First it is not consistent with RCFL standard operating procedures (SOP), contrary to the government's assertion. RCFL's have a "hands off" policy regarding defense testing and equipment. Fischbach Declaration at paragraph 5(a) and 5(b) sub (c). If the government is in control and custody of the equipment containing defense work product, the government would be able to see the examination progress each time they log Mr. Fischbach back into the system. As Mr. Fischbach writes: "A technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct." *Id*. at 5(a). Moreover, time-tested industry-practiced methodology requires the initiation of certain hardware and applications on each work-station prior to testing and examination, which would necessarily make the observing agent privy to attorney client privilege. If this individual is technically-trained, then he/she can serve can as a conduit of privileged defense information to Mr. Walker. *Id*. at 5(b) sub (b). Mr. Walker has shown a proclivity for relying on information provided by observing Agents,

e.g. Mr. Monroe's recent email describing defense testing personnel in this case on September 25, or procuring a FBI-302 from the Agent observing the defense testing in the *Gonzales* case. The restrictions in paragraphs 6 and 7 of the court's order do not actually make it less likely that the TD software is inadvertently disseminated but they do seriously compromise the security of privileged defense information and data.

Lastly, in paragraph 8 of the court's order at Doc.254 the court limits the defense Internet connection to a single wired Ethernet connection. The factual error here is the assumption that TD software is less secure using a standard WiFi connection, and somehow more secure without the ability of Mr. Fischbach to install industry vetted forensic hardware and software. Were this true then Det. Erdely would have used a wired Ethernet connection himself when conducting his "validation;" but he did not. He used a standard WiFi connection. There is no valid basis to restricting the defense to a wired Ethernet connection which is substantially more expensive and is not available in many places.

Conclusion

The court has found the TD software is material to the defense and that the defense is entitled to conduct independent defense testing. This testing cannot be completed and is impossible without access to multiple ports and network cards. Allowing government Agents to access the computer at start up, perform log in and enter passwords not only affects testing reliability and validity but compromises sensitive and privileged defense data. Lastly, requiring a wired Ethernet connection offers no appreciable security but adds expense to the defense and may not even be available. Attached hereto is a defense proposed Order modifying those paragraphs in the court's order at Doc.254 that addresses these issues so that defense testing is actually possible and can be completed in a safe and secure manner for both the government and the defense.

DATED at Anchorage, Alaska, this 25th day of November 2019.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
Phone 907-277-7171
Fax 907-277-0281
rmherz@gci.net
AK Bar No. 8706023

CERTIFICATE OF SERVICE
I hereby certify that on Nov 25, 2019, a copy of the foregoing Def M for Partial Reconsideration was served electronically on Assistant United States Attorney's Office s/ Robert Herz

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

[PROPOSED] ORDER GRANTING MOTION FOR ADDITIONAL TERMS FOR ROTECTIVE ORDER

Having duly considered the United States' Motion for Additional Terms for Protective Order and Notice of Compliance with Supplemental Order (the "Motion"), the Court ~~grants the Motion and ORDERS that:~~ denies the government's motion at Doc.244 but supplements its orders at Doc.231 and 243 as follows:

~~1.~~ ~~The government will provide a computer at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The computer will have one version of Torrential Downpour installed, *i.e.* version 1.23, one of the versions used in this investigation.~~ The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

The government will provide a copy of both Torrential Downpour versions used in this case, i.e. v. 1.15 and v. 1.23 to the defense on either CD/ DVD media or USB solid state or mechanical drive at the Orange County Regional Computer Forensics Laboratory.

The government shall produce at the RCFL both versions of the TorrentialDownpour software, the government's "validation" results, and Det. Erdley's Report no later than November 20, 2019.

//

2. The only persons who will have access to the ~~computer~~ ~~are~~ software are Jeffrey Fischbach and Robert Herz (collectively "the defense"). The defense will have access to the ~~computer~~ software for ~~21 consecutive~~ thirty (30) calendar days of testing.

3. ~~The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.~~

4. The defense may bring digital media, computers, and phones into the room with the ~~computer~~ software.

5. The defense will not remove the ~~computer~~ software from the OCRCFL. The defense will not copy Torrential Downpour.

6. ~~The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape~~.

7. The defense will not download or distribute child pornography ~~using the computer~~. Any downloading of child pornography would constitute a violation of the federal criminal code.

8. ~~All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain~~

the Wireshark data pending further order of the Court.

9. At the conclusion of testing, the FBI will "zip" all the Wireshark files, meaning it will use software to compress them. The FBI will "hash" the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government may provide the computer by November 20, 2019. The government's compliance with this Order satisfies the government's obligations under United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).

Moreover, the Court reaffirms its prior protective Order (Dkt. 231), as follows:

Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person

without prior order of the Court.

Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this case, provided the materials are filed under seal and/or submitted to the Court for in camera inspection.

Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

DATED this _____ day of November, 2019, at Anchorage, Alaska.

_____
UNITED STATES DISTRICT COURT JUDGE

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America, Plaintiff, vs. Matthew Schwier, Defendant.	)	Case No. 3:17-cr-0095 SLG-DMS

DECLARATION OF JEFFREY M. FISCHBACH
IN SUPPORT OF DEFENSE MOTION FOR RECONSIDERATION

I, Jeffrey M. Fischbach, declare as follows:

1. In its "ORDER RE MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER (Dkt. 254)" the court has demonstrated clear efforts to strike a balance between the need for the defense to complete tests which the court has found to be material, with the government's concerns regarding *potential* distribution of its proprietary software. However some government language adopted by the court, makes it impossible for me to conduct the tests which the court has found are material to the defense. Mr. Walker himself, has admitted that the arbitrary limits he has asked the court to adopt, *do not* actually serve to prevent the government's software from "escaping into the wild". Specifically, the government's arbitrary constraints on how I physically can and cannot access the government's own equipment prevents me from conducting the defense tests that I must complete for trial. I do believe, however, that this may be a simple misunderstanding of the software and equipment necessary

to complete testing and subsequent analysis.

2. Without unfettered access to computer ports, in order to install my own tested, industry-accepted software and hardware, as well as to remove my test results from the government provided computer for further examination and analysis at my laboratory, I simply can't complete the tests that the court has found material to this matter. With current restrictions in place, I can't even connect a screen, keyboard, or mouse, let alone the hardware and software that I need for my tests, and that are required by industry standard forensic practice in order to insure that no data accidentally alter my results or escape the system. As Agent Allison should well know, some of the most effective industry-tested forensic standard software *requires* a USB dongle (key) to remain plugged into the computer's USB port, in order to use the software. Indeed, this USB key was necessary and *required* for Allison to use the software he relied upon in his own work to forensically examine the evidence seized from Mr. Schwier's property. The very same software that produced results inconsistent with TD. Thus, had Agent Allison been subject to Mr. Walker's restrictions of only connecting to one network card port, even he could not have completed his own exam which alerted the defense of these inconsistent findings.

3. If Mr. Walker isn't aware that his arbitrary restrictions limit my work to only reproducing Mr. Erdely's "validation" procedures, then he simply hasn't done his homework or consulted with his own experts. This not only restricts me only to performing Mr. Erdely's "validation" procedures, but it doesn't even allow me to competently utilize the tools available to me to personally assure that no unintended data enters or exits the machine, as Mr. Walker himself claims to fear. I see no scientific or investigative value to utilizing precious resources repeating Mr. Erdely's "validation" here in California. On the contrary, I refuse to be associated with the propagation of "junk science", as dictated by an apparently biased actor, who clearly doesn't understand scientific method or computer security.

4. To a significant degree, the court relied on the government's [PROPOSED] ORDER GRANTING MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER filed on

November 18, 2019, which was little more than a superficial makeover of their prior proposal which *only* served to allow me to perform ***their*** proposed "validation", and not my tests. It appears to me that the court was able to recognize that tests conducted under the government's own prescribed "validation" procedures would effectively neutralize decades-old practices of independent review. The court's current order seems to address *most* of those arbitrary government constraints.

5. In order to clearly articulate for the record why I am unable to effectively prepare counsel for trial with certain remaining restrictions, I will address my remaining concerns within Dkt. 254 line-by-line in the following paragraphs. Paragraph numbers in **bold** reference and correspond to the numbered paragraphs in the court's order at Doc.254.

a. ***(Paragraph 6)*** *Government personnel will have access to the TD Computer only for the purposes of starting the TD Computer, entering the password for the defense, and keeping the TD computer secure consistently with OCRFCL standard operating procedures. Government personnel will not observe the defense testing.*

Rather than relying on AUSA Walker's self-serving interpretation of OCRCFL standard operating procedures, I would urge the court to compel Mr. Walker to produce text from the actual SOP upon which he claims to be relying. Based on his insertion of government personnel into a defense examination, I don't believe he has even consulted the RCFL. I have personally utilized several RCFL facilities around the country. Contrary to Mr. Walker's representation, it has been my experience that RCFL personnel have been instructed specifically *not* to interact with equipment used by the defense, specifically because doing so risks physically observing privileged work product, and can lead to accusations of government "snooping".

In this particular case, Mr. Walker has *already* asked the OCRCFL's Joseph

Monroe to provide details about my examination. Should Mr. Monroe, (or other RCFL staff) be in control and custody of the equipment containing my work product, they would be able to see my examination progress each time they have to log me back into the system (which happens every time I so much as leave to use a restroom), as well as hold exclusive possession of the password to access it while I am away, he (they) would most certainly be suspect, should my tests or the computer fail, or should the government appear to gain advanced knowledge of my testing results. While this may not have previously been as great a concern when Mr. Reardon was assigned to the case, it has been of particular concern given Mr. Walkers already proven proclivity to use RCFL staff, with no apparent justification, to provide information about my examination, communication, and consultation. While I do understand that the AUSA does have the power to use the RCFL in this way, I seriously doubt that it is the court's intention for him to continue do so.

Any government access to my tests and/or testing environment (hardware/software), including set-up, risks attorney-client privilege and work product, my ability to authenticate my own work, inserts the government into the defense chain-of-custody, and could invalidate my test results. A technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct. The government has not justified how being granted sole password access to my tests, and physically opening the screen every time I need to use the computer, *in any way* serves to secure its software or equipment, (or serves to protect children,) when the equipment itself will already be in the *physical* custody of the government to begin with. Despite his knowledge of the stolen hard drive I reported to Mr. Monroe, Mr. Walker does not so much as specify any need or requirement for well-established forensic software/hardware measures that could be used to *actually* protect the equipment and data (including TD software) against being physically stolen or accessed from the RCFL.

With the physical restrictions pertaining to access to the government computer, noted below in Paragraph 9 of the court's order, which were imposed at the government's request, I can't even install and utilize these standard measures, let alone the software/equipment I need to perform my tests. All of which leads me to believe that either Mr. Walker is simply naive and has not done his homework, or that his real motivation is to thwart my examination of TD software and/or use it to prove that I have in some way violated a court order, so that he can either eliminate or damage my testimony in the defendant's case.

Moreover, in *no way* is *any* of this "consistent with OCRCLF standard operating procedures". This is blatant misrepresentation to the court. Mr. Walker himself provided me the password to the computer currently housed at the OCRCFL. Mr. Monroe, to my knowledge has had *no* access to this password or even touched the keyboard of that machine. This does, however, further justify the need for me to have complete, unfettered control over my equipment, including exclusive password control, not shared with the government, while conducting tests at the OCRCFL

> b. ***(Paragraph 7)*** *Installation of Torrential Downpour software onto the TD Computer will occur as follows:*
>
> > i. ***a.*** *An FBI agent or Task Force Officer will keep exclusive possession of a USB drive or other removable media containing the Torrential Downpour software. The defense will not possess the Torrential Downpour software, other than on the TD Computer.*

I have consistently agreed that the RCFL should maintain custody of the TD installation disk provided to it. As Mr. Monroe himself has conceded, my own equipment which I was required to leave at the OCRCFL, was stolen from the OCRCFL's Defense Exam room, while I was not present, and while in the custody and control of the government. It would certainly be prudent to make sure that this software is kept secure. However, the tests that were ruled material *do* require testing and analysis of TD which *necessarily* requires that I

make multiple copies subjected to industry-tested software and hardware analysis. Therefore, while this can all occur within the confines of the OCRCFL, it simply cannot be completed, *in any way*, on a machine restricted in the way the government has outlined. Again, the government's proposed order simply allows for me to conduct Mr. Erdley's "validation" in California, without Det. Erdely's physical presence.

> ii. ***b.*** *Prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer, all while in the physical presence of the FBI agent or Task Force Officer. The FBI agent or Task Force Officer may observe Mr. Fischbach install the software.*

Mr. Walker has already reached-out to OCRCFL personnel to gain intelligence on my previous examinations and work. Since the passing of the Adam Walsh Act RCFL "Walsh Rooms" (Defense Exam rooms) have been treated as a "firewalled" environment where defense examiners can conduct their work without exposing privilege or work product. The government now seeks to breach this "firewall", which only serves to undermine operational practices that took years to establish. If the government's restrictions are upheld, it could undermine the trust and use of these facilities by defense examiners across the country.

Mr. Erdely's protocols included starting screen capture & monitoring software, as well as Wireshark, *before* the installation and initiation of his software. My time-tested industry-practiced methodology also requires the initiation of certain hardware and applications on each work-station prior to testing and examination, which would necessarily make the observing agent privy to attorney client privilege. At the same time, unless that agent or individual *is* well trained in computer forensics, it is unlikely that he/she would serve *any* value to the government in terms of securing its software. On the other hand, if this individual *is* technically-trained, then he/she serves an even greater value as an "information spy" for Mr. Walker, than in any way to actually secure software.

> ***c.*** *After the installation, the FBI agent or Task Force Officer will remove the USB drive or other removable hardware from the TD Computer.*

The government should continue its now long-standing practice of having a *hands-off* policy when it comes to defense forensic examinations. As I have continued to offer, I would encourage the safe custody of the original software in government hands, and I would be willing to personally put it *in* the government's hands the moment I have completed my use of the installation files. More significant in this paragraph, however, is the government's continued use of the term "TD Computer". This further emphasizes that the government intends for me to operate *exactly* as Mr. Erdely's "validation" protocols specify -- not according to my own testing protocols, that this court has already ruled are material to the preparation of the defense in this case. This notion of a "TD Computer" is simply because Mr. Erdely's protocols specify one computer as "TD", and the other as "Suspect". As outlined previously in my redacted declaration, that is not my proposed operating procedure. And that *will not* allow me to complete the tests that have been found to be material in this case.

> ***d.*** ***(Paragraph 8)*** *The defense may bring digital media, computers, cell phones, and an internet hotspot (i.e. one that is compatible to connect to the TD Computer via the network card) into the OCRCFL room with the TD Computer.*

Again, the government sees fit to dictate the defense examination environment, in order to restrict defense testing to its own "validation" protocols. In this case, however, the government is dictating an Internet connection method (Ethernet) that is currently unavailable on most Cellular 4G hotspots, and one that was not even an option on the WiFi hotspot that Mr. Erdely used for his own "validation". If a WiFI connection is unsuitable, or vulnerable, then it begs the question: why did Mr. Erdely use WiFi himself? I suspect that this government proposed requirement was made simply because it is well known that

there are very few "hotspots" for sale that have a wired Ethernet connection, and that those would be very costly for the defendant. For example, a simple search will show that the only Ethernet-equipped hotspot available from Verizon costs more than 4X as much as a comparable WiFi hotspot from Verizon. ($649.99, compared to $149.99.)

> ***e. (Paragraph 9)*** *The TD Computer will contain one network card. The defense will not make any connections to the TD Computer other than through the network card. The TD Computer may access the internet through the network card.*

As stated above, the government seeks to narrow the defense testing and examination to its own "validation" procedures. In order to complete the tests that have been deemed material, I simply *must* have the ability to connect my own equipment, install my own industry-tested and accepted software and hardware, and to have the ability to remove my results for further examination and analysis. Otherwise, I *cannot* complete the testing that has been found material in this matter. In short, I need access to multiple computer ports and network connections to run my tests.

> ***f. (Paragraph 13)*** *The defense will not tamper with or open the TD Computer.*

I understand and concur with the apparent *spirit* of this paragraph, I would for all of the reasons stated above, ask that the court impose the same admonition on the government. To that end, I had previously considered "tamperability" in my prior equipment specifications *estimate* that was provided to the government last week. Although a desktop machine is considered to be easier and less expensive to repair and upgrade, and has always remained my preferred platform for that reason, I would likely seek to use a laptop for my tests, because while retaining similar capabilities, they are significantly more difficult to alter, and much easier to identify any tampering that has occurred. For several reasons (which I can provide, if necessary, in a redacted document), including this, I tend to rely on Apple laptops, when an examination requires leaving equipment in government custody. At little-to-no added cost compared to similarly-

equipped desktop machines, I believe these safeguards serve to protect and authenticate chain-of-custody, work-product privilege, as well as *both parties* from any associated accusations.

6. I have been working with sensitive files for a quarter-century. Many of the procedures used by the FBI today were first used and instructed by *me*. So long as I have complete and unfettered access to properly determine and configure the equipment I use for these tests, I will take all the aggressive file containment protocols that I *always* use when examining sensitive material. This however, will necessarily require me to configure all equipment myself, and have access to add and remove all necessary software as my time-tested and industry-accepted protocols dictate, which means I will need access to more than one port on the government provided computer and more than one network connection. If I am allowed to do this I can safely *guarantee* the TD software will not be accidentally copied or distributed while under my control. Should I be required to use the computer as dictated by the government, without the ability to install or connect any previously tested and industry accepted software (much of which is specifically designed to protect data from any unintended use) and hardware to *any* port or connector on the computer, as needed, then not only can I not complete my tests, I would not be able to assure the court that all standard precautions had been taken. Given the necessary access I need on the testing equipment provided by the government, I will take all necessary software and hardware precautions to restrict copy or dissemination of TD, and to secure my forensic work environment, as has been my standard practice for 25 years.

7. The foregoing statements true and correct to the best of my knowledge, and I hereby reserve the right to amend them should additional information be made available to me at a later date.

/ / /

/ / /

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on November 25, 2019.

_____

Jeffrey M. Fischbach

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	CASE NO. 3:17-cr-00095-SLG
	)	
MATTHEW WILLIAM SCHWIER,	)	
	)	
Defendant.	)	

PARTIAL TRANSCRIPT OF HEARING ON MOTIONS FOR RECONSIDERATION (1:36 p.m. - 1:47 p.m.)
BEFORE THE HONORABLE SHARON L. GLEASON, DISTRICT JUDGE
November 26, 2019; 1:09 p.m.
Anchorage, Alaska

FOR THE GOVERNMENT:
Office of the United States Attorney
BY: JONAS M. WALKER and CHARISSE M. ARCE
222 West 7th Avenue, #9
Anchorage, Alaska 99513
(907) 271-5071

FOR THE DEFENDANT:
Law Offices of Robert Herz, P.C.
BY: ROBERT M. HERZ
431 West 7th Avenue, Suite 107
Anchorage, Alaska 99501
(907) 277-7171

SONJA L. REEVES, RMR-CRR
Federal Official Court Reporter
222 West 7th Avenue, #4
Anchorage, Alaska 99513
Transcript Produced from the Stenographic Record

(Call to Order of the Court at 1:09 p.m.)

(Proceedings took place that are not included in this Partial Transcript, after which, proceedings continued as follows:)

THE COURT: I understand that perspective. All right. Thank you.

Mr. Herz, go ahead, please.

MR. HERZ: Thank you, Your Honor. And I can put Mr. Fischbach on if necessary, but I think I can summarize our position. If the Court needs clarification from Mr. Fischbach, we can offer it.

A couple of things. I think the Government's issue regarding the Wireshark they have indicated is moot, and I think our point, or the point Mr. Fischbach was making about, quote-unquote, being able to take Torrential Downpour while Wireshark is running wasn't a threat, it was an illustration that the Government's proposed prophylactic using Wireshark just to determine if a copy was made is really ineffective.

So their goal in using Wireshark would not be met by using Wireshark. Essentially, unless Wireshark was being run each and every day of the 21 days and only if each day, after each day's testing the Wireshark packets were examined, that would be the only way the Government would know if a copy got made.

If after 21 days of testing it was never examined, I mean the Wireshark packets were not examined, then only two possibilities can occur. The Government seeks to review the packet captures before trial, in which case they have now discovered attorney work product, protected information and have discovered attorney-client information in advance of trial, which they are not entitled to do. Or the alternative is they wait until after the trial is complete and then they want Court permission to examine the packets to see if copying was made, at which point it's really after the fact.

At that point, if there was copying done, we didn't do anything to prevent public dissemination of the software, it's really now being used as evidence to see if some illegal conduct occurred. So as a prophylactic measure, it really doesn't serve the function that the Government states it would serve.

THE COURT: Mr. Herz, let me interrupt on that, because I thought I addressed this in the order as well, and that is that if there isn't Wireshark or another type of capture device used, I don't see that Mr. Fischbach would be able to testify because of the Daubert issues. I thought I was fairly explicit on that, maybe in a footnote, but to establish reliability

-- and Mr. Fischbach has acknowledged this repeatedly.

What I would truly hope to -- so if there is going to be testimony, then I do intend to order full discovery of the expert prior to trial, even if the existing rule doesn't expressly contemplate that, it will on December 1st I believe. There is going to be a rule change to 16 that would make that clearer. So that's my intent is if it's going to be used at trial, it is fully discoverable, just as I would expect and I understand the Government has made there.

So I wanted you to have that heads-up that based on the evidence I have heard from both of the experts, it is extremely improbable that a reliability standard under Daubert could be established by Mr. Fischbach without a capture of the work product. So heads up on that.

MR. HERZ: Okay. I appreciate that, Your Honor. And I guess we can take that up -- that issue up when it arises, but just as a prefatory response, there is no other area of science where the reliability of the science is dependent on audio and video recording or capturing of the actual testing.

Normally the reliability standard is addressed simply by the expert testifying about the procedures, the scientific procedures that were utilized in

conducting the tests. And that's true when an expert in DNA testifies about what procedures they used in the laboratory to produce their DNA results. That's typical for hair and fibers.

Nobody's audio and video recording anything. They are simply testifying to standard laboratory procedures. And that's been the case historically even in computer forensics. So I think there are a number of valid and different ways to establish the reliability of testing in computer forensics, not just using a packet capture program.

THE COURT: Well, I'm relying on the testimony of both experts that's been presented. Mr. Fischbach I believe -- well, in any event, heads up on that. I was quite persuaded by the benefits of Wireshark and I tried to flag that issue in the order, footnote three, page two of Docket 254.

All right. Go ahead, Mr. Herz.

MR. HERZ: And we did notice that. Mr. Fischbach and I did speak -- talk to each other about it, so we're well aware of the Court's leanings in that direction.

Regarding computer specifications, the Court's procedure that it outlined actually from the defense perspective makes a lot of sense in that it would be

very helpful to know software specifications and installation instructions, and then we can tailor a defense request regarding specifications.

At this point, what the Government sounds like they are doing is they are putting together a computer based on what their knowledge of the software is and basically saying that should be adequate. So it sounds as though they know what the software specifications are. The problem is they haven't yet shared that with the defense, and we would like an opportunity to be able to give specifications to the Government based on how the software operates, including both versions, not just version 1.23.

And if we don't have that information by tomorrow, our obligation under the Court's order at 254 is that we have to give specifications, and in the absence of knowing specifics about the software, we are very likely going to specify pretty much something very similar to what the Court saw in the e-mail chain and in Mr. Fischbach's latest declaration, because we're unable to specify anything else.

And as Mr. Fischbach did point out, some of the specifications are not simply tailored to the software specifications, but also to the needs of the software and hardware Mr. Fischbach needs to run in order to

complete his tests.

So the specifications we're using take into account two things: One, the software specifications, and, two, the hardware and software Mr. Fischbach needs to use in his testing.

So we're concerned if the Government has an idea about what computer specifications it thinks it would like to provide to us, we would like to know that now so we can respond to that tomorrow by our deadline, or perhaps the Court might want to consider a different schedule for trading information regarding software specifications and computer specifications.

But as it stands right now, we're probably going to specify precisely what we have been talking about in the absence of any additional information coming from the Government.

And so I think the Government has pretty much said that Wireshark is moot, so respectfully I would suggest that that means the motion should be denied. On the other hand, our motion for partial reconsideration simply addresses the fact that the tests that were proposed and that the Court has found to be material cannot be completed with a single network connection and a single port.

And I think Mr. Fischbach made that very clear

in his first declaration that was filed, and so the proposed order we gave the Court eliminates those issues and allows the testing that's been proposed to move forward.

And then specifically regarding multiple copies, perhaps we need to clarify that. The issue involving copies is once Torrential Downpour is downloaded onto the Government-provided computer, it would stay there and any additional copies would stay there, but it's standard computer forensic practice to have a, quote-unquote, "original copy" on the computer on which it's installed, and then to make a second copy or a third copy that you can work on so that you can always have a reference point to make sure that if there are any changes they can be documented, because you don't really want to create by accident any changes.

You need to be able to make sure that what you're working with is in its original condition, so you need an original copy and then you need a working copy essentially. And I think Mr. Fischbach can explain that in more detail if the Court would like, but he's not talking about making multiple copies outside of the Government-provided computer domain. All of it stays on the Government computer, none of it goes anywhere else. It's just simply creating working copies, which is

standard forensic practice.

(Requested excerpt concluded, proceedings continued.)

CERTIFICATE

I, Sonja L. Reeves, Federal Official Court Reporter in and for the United States District Court of the District of Alaska, do hereby certify that the foregoing transcript is a true and accurate transcript from the original stenographic record in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

Dated this 10th day of December, 2019.

/s/ Sonja L. Reeves
SONJA L. REEVES, RMR-CRR
FEDERAL OFFICIAL COURT REPORTER

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America, Plaintiff, vs. Matthew Schwier, Defendant.	)	Case No. 3:17-cr-0095 SLG-DMS

SUPPLEMENTAL DECLARATION OF JEFFREY M. FISCHBACH IN SUPPORT OF DEFENDANT'S MOTION FOR PARTIAL RECONSIDERATION AT DOC.256

I, Jeffrey M. Fischbach, declare as follows:

1. In its most recent motion at Doc. 255, the government continues to attempt to impose its self-serving protocols on the defense. This motion, in one stroke, serves to limit the defense to *only* being able to conduct Mr. Erdely's own "validation", and prevents the defense from completing its own tests, which the court has already ruled are material. The government's sole assertion justifying its purported need for Wireshark is to prevent the accidental copying or distribution of its TD software. Implementing the use of WireShark does *nothing* to *actually* prevent the accidental or intentional distribution of its proprietary software. I would also note that, here again, the government makes no effort to even feign concern for potential harm to children -- commensurate with the charges. As such, the government continues to allow me unfettered access to

alleged child pornography *faciliated* by AUSA Jonas Walker, without so much as a protective order, while he continues to urge the court to impose arbitrary limitations on my ability to conduct tests, which even Walker himself, admits *do not* actually serve to prevent its software from "escaping into the wild".

2. Specifically, I agree that Wireshark is a very useful tool to observe any nefarious *or* legitimate use of any computer computer IO (input-output) port, including wireless. Since I agree to this premise, it would seem the government's need to call a witness is unnecessary just to testify to this fact. The government makes no assertion that Wireshark does *anything* to prevent the copying of its software. The fact is that it does not. Its only function is to record the transmission and receipt of data on the host device. According to Wireshark's own website: *"What is Wireshark? Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network."* (https://www.wireshark.org/faq.html#_what_is_wireshark). I agree that Wireshark -- if configured to do so, and if started, and if it is left uninterrupted, *by me* -- will record the [accidental] copying of TD. But only if all those things happen, and only if *I* allow that action to be recorded. What it will also record is *every single element of my testing*, as data is transmitted for testing purposes, moment-by-moment, in exhaustive detail. And the only way Mr. Walker will have the ability to even make the accusation that TD has been "released to the wild", intentionally or accidentally, will be for him, or more likely, someone working for him, to decrypt and analyze my detailed recorded work product -- if so ordered by the court. And in doing so the government will have accessed attorney-client privileged data and obtained protected attorney work product information.

3. I am arguably one of the best equipped people on the planet to steal this software without anyone ever being the wiser. And I can do it *while* Wireshark is running. Now after questioning my credentials for almost two hours on the stand, Mr. Walker has pivoted to his "concern" that I might "accidentally" copy the

software. Perhaps Mr. Walker is prone to accidentally copying or deleting files on his own computer, but I have been working with sensitive files for a quarter-century. Many of the procedures used by the FBI today were first used and instructed by *me.* So long as I have complete and unfettered access to properly determine and configure the equipment I use for these tests, I will take all the agressive file containment protocols that I *always* use when examining sensitive material. This however, will necessarily require me to configure all equipment myself, and have access to add and remove all necessary software as my time-tested and industry-accepted protocols dictate, which means I will need access to more than one port on the government provided computer. If I am allowed to do this I can safely guarantee the TD software will not be accidentally copied or distributed while under my control. Should I be required to use the computer as dictated by the government, without the ability to install or connect any previously tested and industry accepted software (much of which is specifically designed to protect data from any unintended use) or hardware to *any* port or connector on the computer, as needed, then not only can I not complete my tests, I would not be able to assure the court that all standard precautions had been taken.

4. Mr. Walker brings to the court's attention the theft of a hard drive I left in the *government's* custody, care, and control. In what can only be referred to as an opportunistic loose association with truth, Mr. Walker makes the unsubstantiated and false claim that "Mr. Fischbach has, already, *lost* a hard drive at the OCRCFL in this case." Mr. Walker is well aware, via his intrusive interrogation of my assigned RCFL liaison, Joseph Monroe, that Mr. Monroe did not describe my hard drive as being "lost". He described it as "missing" from the Defense Review room, where I am *required* to keep it, in order to allow me to continue processing data overnight or over the course of several days. Which, in order to complete my work for trial, without delay, is both necessary, and facilitated by the RCFL. Mr. Monroe has documented by email, dated July 2, 2019, his knowledge that the

processing (long periods of time the computer works without examiner input) of my examinations were ongoing, in my absence. He specifically requested my permission to allow someone to disconnect the equipment, in order for another examiner to use some of it. In an email from Mr. Monroe, solicited by Mr. Walker, documenting his observation of my examination, Mr. Monroe wrote the following: *"Only Fischbach and Herz came back on 25th. Fischbach advised he was missing an external hard drive that he left in the Defense Review room, during his last visit. We were unable to locate the missing external hard drive."* As Mr. Monroe was aware, that drive was connected to the *government's* work station -- as it was when the work-station was in Anchorage, supervised by Kyle Reardon.

5. Despite my request to use two *significantly more* secure private exam sites -- FBI Wilshire, and Roybal Federal Court's SCIF, both of which I have successfully used many times without incident, and both of which are *significantly* shorter drives for me -- it is Mr. Walker who has insisted that I use the OCRCFL, where he is, apparently, able to maintain a closer watch on my work, and with whom I work. Mr. Walker should know, however, that unlike the FBI and LA SCIF, the OCRCFL offers *only* a shared work space where many different civilians and RCFL personnel come and go and even share much of the same equipment. I would agree that the OCRCFL is a location that *does* risk the possible theft, not only of TD, but of the *entire computer* upon which it is installed. Frankly I am surprised, given the government's purported concern about the security of its TD software that it has not readily accepted my offer for the defense testing to occur in the federal court SCIF. Not only can the OCRCFL not guarantee that items will not be stolen from its own Defense Exam room, it apparently does not take seriously its role in protecting details concerning the use of its defense work environment from the government. What Mr. Walker does not know from his heretofore unjustified intrusion into my RCFL work is whether the

missing drive, taken from the RCFL Defense Review room, when I was not present, was encrypted to secure its contents so that only I could personally decrypt them, or whether that encryption was set to wipe the drive upon unauthorized attempts to open it, or whether the drive had tracking measures installed, or whether that drive has since been found and returned to me thanks to any of the above measures. While Mr. Walker does not have an explanation for how Wireshark *in any way* prevents the theft or accidental copying of its software, (which it emphatically does not,) I can assure that court, given unfettered access to *all* testing equipment, that I *will* guarantee that, in my hands, the software will not escape the OCRCFL. I cannot, however, make the same guarantee for the TD copy the court's order requires be left with FBI or OCRCFL personnel.

6. Much like Mr. Walker knew that Internet access was *required* to test Torrential Downpour, he also knows that it was the RCFL that "lost" a hard drive left in *their* care. He also knows that in order for Wireshark to be used in the way he proposes, I would have to be *trusted,* unmonitored, by myself, to actually configure it the way he wants me to, and to use it, without interruption or log file alteration, to record *all* of my activity on the computer the government will provide. Moreover, like the TD secrets already accidentally exposed to me, and the missing hard drive I reported to the OCRCFL, the only way that the government would even know that their software escaped the RCFL lab is either if *I* can be trusted to report it to them, or if they actually plan on arbitrarily demanding the examination of the Wireshark recording they trusted *me* to make. By which time, given their self-imposed requirements, the software would be irretrievably lost to "the wild". On the other hand, examination of these Wireshark logs by the government would give them a very complete reenactment of my tests; tests protected by attorney-client privilege and attorney work product doctrine.

7. As noted by the government, the court ordered, "On or before Monday,

November 25, 2019, the government will provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements." And that, "Not later than Wednesday, November 27, 2019, the defense shall provide to the government the specifications for the computer that it is seeking for TD testing." The court clearly understands my limited ability to determine appropriate specifications for the hardware and equipment I need to test the software, without first being provided any documentation or specifications relating to the software to be tested. In its motion at Dkt. 255 the government has instead chosen to ignore the court's order to provide complete documentation and equipment specifications, and ignores, as well, the equipment specifications I already provided without the benefit of the materials now ordered by the court. Mr. Walker instead has seemingly made the arbitrary decision to provide a piece of used equipment, similar to the vintage equipment it has already provided to the OCRCFL without any reference to the specifications provided to him by the defense already. Mr. Walker has nowhere in Dkt. 255 explained why the court's order to provide TD documentation and equipment specifications is unreasonable or untenable. He simply seems to believe that his judgment of what I need to complete my tests supersedes either the court's or mine.

8. As such, the government has <u>not provided installation instructions or minimum operating requirements</u>, (per my previous requests, or the court's order), with its heavily redacted TD User Manual for version 1.23. At Mr. Walkers request (November 19, 2019 email), the following equipment estimates were provided: Apple Macbook Pro Laptop, 2.8GHz quad-core Intel Core i7

processor, 64GB memory,, 512GB SSD storage, Thunderbolt / USB-C, WiFi/RJ45. (Updated and summarized here.) While outwardly similar to the equipment Det. Erdely used to perform his "validations", this equipment was specifically chosen, with the expectation that, while accommodating the operating system and software I was able to *observe* Erdely using for his "validations", it should also provide an environment that will accommodate the forensic hardware and software I need to install in order to both complete my testing and assure the court that the machine has in no way been compromised during my testing, and that no software or data has been lost, stolen, or compromised. This hardware has some other very specific capabilities which are routinely utilized by forensic technologists, that are both necessary to complete my tests in time for trial, as well as to secure the equipment, software, and data from theft, intercept or alteration. While it is my usual practice to consult software specifications before choosing hardware, in the absence of court-ordered specifications, *this* hardware is suited to accommodate my anticipated needs for TD testing, as described previously to the court, while allowing me to use industry-standard practices to protect the software, data, and equipment. The equipment Mr. Walker has described in Dkt. 255, is not.

9. The court's order for documentation materials, quoted above, is in no way ambiguous or silent to its documentary requests, nor does it speak to any redactions. Mr. Walker previously claimed, while on record, that no such documents exist, but now he says they need to be redacted. Similarly, after affirming to the court that software change logs did not exist, they suddenly do.

10. The court order to "provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and

minimum operating requirements," is clear and unambiguous. However, as he has done previously in this case, Mr.Walker is again opportunistically interpreting the court's lack of granular specificity to mean "redacted" material, as the government sees fit to define "privileged information". Again, I remind the court that Mr. Erdely stated under oath that TD's secret identity was it's *only* secret. Yet the government continues to claim that there are other things which the defense should not be able to see. One of those things may be responsible for the reason that TD investigations across the nation have, on several occasions, been inconsistent with the findings of well-tested, industry accepted software and hardware. As is the case herein.

11. Given the necessary access I need to complete my testing on the equipment provided by the government, I will take all necessary software and hardware precautions to restrict copy or dissemination of TD, and to secure my forensic work environment, as has been my standard practice for 25 years.

12. The foregoing statements are true and correct to the best of my knowledge, and I hereby reserve the right to amend them should additional information be made available to me at a later date.

/ / /

/ / /

/ / /

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on November 25, 2019.

Jeffrey M. Fischbach

Robert Herz

From: Robert Herz [rmherz@gci.net]
Sent: Friday, December 06, 2019 5:04 PM
To: 'Walker, Jonas (USAAK) 5'
Cc: 'Jeff M. Fischbach, ABFE'
Subject: RE: Hardware and software Specifications

Mr. Walker,

I would agree that Mr. Fischbach is in the best position to know what his needs are in order to conduct defense testing of the TD software. As such, Mr. Fischbach has concluded his inspection of the system requirements of the laptop supplied by the FBI, and it will not be sufficient to meet defense testing needs. It is a 2014 vintage A1398 MacBook Pro, with minimal speed and memory, and outdated hardware and port specifications. Similar to the machine currently in use at the RCFL, it is unlikely that this laptop also will not support running the Virtual Machines supplied by Mr. Erdely. This machine was the least powerful configuration of MacBook Pro produced in 2014. But, is far slower than the minimum requirements of today's Macs. Notably, at this juncture the Government is seeking an order that Mr. Fischbach only use an Ethernet port. This machine does not have an Ethernet port.

The following are the *minimum requirements* needed in a government supplied machine necessary to conduct defense testing of the TD software. Defense specifications are in black, corresponding specifications of the computer supplied by the government are in red:

2.6GHz 6-core 9th-generation Intel Core i7 processor (4-core 4th generation processor discontinued in 2015 nearly five years ago)

64GB 2666MHz DDR4 memory (16GB 1600 MHz DDR3 -- incapable of additional RAM)

AMD Radeon Pro 5500M with 8GB of GDDR6 memory (2GB discontinued graphics processor)

512GB SSD storage (Unknown)

Thunderbolt / USB-C (No USB-C)

WiFi & RJ45 Ethernet (No Ethernet)

The Mac laptop also must have Bootcamp & **valid** Windows 10 installed.

Please let me know when a machine with these minimum requirements will be supplied and available for Mr. Fischbach's use.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Friday, December 06, 2019 3:31 PM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Arce, Charisse (USAAK) 1; Russo, Frank (USAAK); Allison, Daryl (AN) (FBI)
Subject: RE: Hardware and software Specifications

Mr. Herz:

Thank you for contacting me regarding you concerns.

Per my email of 12/4 below, the government believes that the computer provided is sufficient to run TD as it would be used in an investigation.

The government does not know what tests Mr. Fischbach intends to run, as the defense has withheld that information from the government. Without knowing what tests Mr. Fischbach intends to run, and the technical requirements of those tests, the government is not in a position to opine regarding what technical specifications are necessary to meet Mr. Fischbach's needs.

Because Mr. Fischbach has access to the technical specifications of the computer, as described below, Mr. Fischbach is the person best situated to answer your question regarding whether the computer is sufficient to run Mr. Fischbach's tests.

Thank you,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Friday, December 6, 2019 2:56 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: Hardware and software Specifications

Mr. Walker,

I agree the court stayed the requirement that the government does not need to provide the TD computer. But the court did not stay the entire order at Doc. 254. As such, the requirement that the government provide all software documentation related to TD is still binding on the government.

Moreover, I believe this was in recognition that the defense needs the TD software specifications in order to provide a tailored request for computer specifications for the computer that the defense needs to runs its tests. Nevertheless, the government prior to knowing what the defense specifications would be, "selected" a computer that the *government believes* the defense should use. This was not the process the court envisioned by its order at Doc.254 and seems a bit "cart before the horse." Given that Doc.254 was not stayed in its entirety, I disagree that the government has complied with the court's orders, or that the court's orders have been exceeded. That Mr. Fischbach is attempting to ascertain the system requirements of the computer the government provided, prior to defense input, only means we are evaluating what has been sent to see if it will meet defense needs. Our preliminary review suggests that it will not be

adequate. When Mr. Fischbach completes his work at the RCFL later today, I will provide the government notice of what specifications are, in fact, needed, and whether the computer sent prematurely will meet defense needs. However, the lack of TD software specifications has significantly hampered the defense in this evaluation.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Thursday, December 05, 2019 5:44 AM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Monroe, Joseph; Allison, Daryl (AN) (FBI); Steeves, Holly J. (AN) (FBI); Arce, Charisse (USAAK) 1
Subject: RE: Hardware and software Specifications

Mr. Herz:

Good morning. I replied in a separate email chain regarding the defense request for Mr. Monroe to show Mr. Fischbach the computer settings. As indicated, I don't object to that request, and I appreciate Mr. Fischbach's suggestion that he see the settings in person to get the data he needs. That seems like an efficient way to get the data directly to Mr. Fischbach.

At Dkt. 262, the court vacated the order at Dkt. 254 in that the government does not have to provide the TD computer to Mr. Fischbach at this time.

Also in Dkt. 262, the court ordered the defense to provide specifications by 12/6. To assist the defense in this process, I provided the specifications of the selected computer in a prior email chain yesterday; see below, immediately prior to your email.

Accordingly, the government has complied with the Court's orders, and, in fact, has exceeded them, in that Mr. Monroe will be showing the computer details to Mr. Fischbach, which is what Mr. Fischbach requested.

The Court will, no doubt, appreciate the parties' cooperation regarding these technical details.

Thank you,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Wednesday, December 4, 2019 2:49 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: Hardware and software Specifications

Mr. Walker,

Unfortunately, this is insufficient information to allow the defense to make a determination whether this machine will be adequate for defense testing purposes. Will you allow Joe Monroe to boot up the computer on Friday in Mr. Fischbach's presence so that more specific information can be obtained about what has been sent?

In addition, does the government intend to provide more and complete information regarding TD software specifications before this Friday, and as required by the court's order at Doc.254?

Thank you for your attention to these requests.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Wednesday, December 04, 2019 12:41 PM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Allison, Daryl (AN) (FBI)
Subject: RE: Hardware and software Specifications

Mr. Herz:

I am advised that a computer with the following characteristics has been identified, which the government expects to be sufficient:

Apple MacPro laptop with Windows 10 Pro loaded on Bootcamp partition Laptop has 16GB of RAM, 64-bit Operating System x64 based processor with a 250GB Hard Drive

Thank you;

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Tuesday, December 3, 2019 11:41 AM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>

Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: Hardware and software Specifications

Mr. Walker,

At Doc. 262 the court ordered the defense to provide the government with the computer specifications the defense deems necessary to allow defense testing of the TD Software on a computer the government will provide for defense testing. Based on information provided to the government in email correspondence, pleadings, and declarations, the defense has made it clear that hardware specifications are predicated in part on the software the computer will run, meaning that it is important to know the specifications of the TD software. Ultimately, defense computer hardware specifications will be based on TD specifications as well as the various software Mr. Fischbach will install and that are needed for defense testing. The court ordered the government at Doc. 254 to provide the defense "with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements." To date, the government has provided only a user manual for TD version 1.23, and it was redacted. This does not comply with the court order, and prevents the defense from more meaningfully providing computer specifications to the government by this Friday. The defense has provided the government with specifications recently in Mr. Fischbach's declaration at Doc. 261 para.8. The defense believes that the court intends for the parties to refine these specifications which is why the court changed the defense deadline to December 6. If the parties are to refine the specifications as the court intends, then the government must provide TD software specifications as directed in the court's order at 254, which in turn will allow the defense to make a more refined and tailored request concerning computer specifications. If the government is not willing to fully disclose software specifications to both TD versions in a timely manner and *before* Friday, which is necessary to allow for defense review and evaluation, then the defense will be unable to refine the specifications previously provided to the government, and those previously provided specifications will stand as to what the defense will be requesting.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

Robert Herz

From: Walker, Jonas (USAAK) 5 [Jonas.Walker@usdoj.gov]
Sent: Wednesday, November 20, 2019 1:45 PM
To: Robert Herz
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Is the defense requesting testing using the computer already at the OCRCFL?

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Wednesday, November 20, 2019 1:33 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

We are trying to get this done, and proceed to trial, while placating your fear of "the wild." If you speak with your own experts, I'm sure they can explain to you how virtual machines work, and I'm even more certain that they can tell you exactly what specifications are necessary to install and run TD. Alternatively, you could provide those to Mr. Fischbach, as I have already requested. If you are informing me that you already have personal knowledge that there is no way for Mr. Fischbach to use the computer at the RCFL to install and operate TD, then please provide a computer either with the specifications that are required by the software, or with the hardware/software specifications you requested from me, that I have already provided to you.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Wednesday, November 20, 2019 11:16 AM
To: Robert Herz
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Per your email below, is the defense requesting testing using the computer already at the OCRCFL?

The computer already at the OCRCFL doesn't have internet access. Also, the TD Computer would likely be wiped prior to TD installation.

Thank you,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Tuesday, November 19, 2019 11:49 AM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

Because Mr. Fischbach was able to observe the vintage of the Mac used for "validation", he believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation -- thus assuring the government that no copy will be placed on his own equipment. Because his testing protocols do not require any interaction with contraband, he will use his own equipment to interact with TD installed on the computer at the RCFL. Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions. If, however, Mr. Erdely can supply such information, or is able to render an opinion regarding the equipment provided to the RCFL by the AUSA, it would certainly save the loss of valuable time if Mr. Fischbach could be made aware of any limitations prior to beginning his tests.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Tuesday, November 19, 2019 9:04 AM
To: Robert Herz
Subject: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Good morning.

In Dkt. 249 at 10, Mr. Fischbach wrote: "Towards that end I am amenable to the government providing to me a computer configured to my specifications. In order to assure scientific results, I have to personally conduct the installation of any software to be tested."

Please promptly advise what "specifications" Mr. Fischbach is requesting.

Thank you,

-Jonas M. Walker
Assistant United States Attorney
District of Alaska
907.271.3983

Robert Herz

From: Robert Herz [rmherz@gci.net]
Sent: Tuesday, November 19, 2019 2:45 PM
To: 'Walker, Jonas (USAAK) 5'
Cc: 'Jeff M. Fischbach, ABFE'
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

Mr. Fischbach says that because he still has not been provided with any TD documentation and other materials that would be typically provided to a user of TD, he would only be able to specify the most robust desktop equipment available to a forensic professional at this time. If you would like to provide TD documentation materials he may be able to give you a more concise specification, and thus save time and money.

However, at this time, given the ambiguity of the software requirements, he can only specify a currently robust (but by no means server-level) workstation. Again, it would be more productive for all concerned, if we simply had a copy of the software specifications. The specifications below are only minimum estimates for TD -- not for his complete testing. For practical, and defense privileged purposes, he will use his own equipment as a testing component, but will not install or copy TD to any of his own devices.

2.6GHz 6-core 9th-generation Intel Core i7 processor
64GB 2666MHz DDR4 memory
AMD Radeon Pro 5500M with 8GB of GDDR6 memory
512GB storage
Thunderbolt / USB-C
WiFi & RJ45 Ethernet
Mac must have Bootcamp & valid Windows 10 installed.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Tuesday, November 19, 2019 12:14 PM
To: Robert Herz
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

I appreciate the prompt response.

Other than agreeing to use the existing computer, what "specifications" does Mr. Fischbach require, per Dkt. 249 at par. 34?

Thank you,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Tuesday, November 19, 2019 11:49 AM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: US v. Schwier: specifications question re: Dkt. 249

Mr. Walker,

Because Mr. Fischbach was able to observe the vintage of the Mac used for "validation", he believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation -- thus assuring the government that no copy will be placed on his own equipment. Because his testing protocols do not require any interaction with contraband, he will use his own equipment to interact with TD installed on the computer at the RCFL. Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions. If, however, Mr. Erdely can supply such information, or is able to render an opinion regarding the equipment provided to the RCFL by the AUSA, it would certainly save the loss of valuable time if Mr. Fischbach could be made aware of any limitations prior to beginning his tests.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Tuesday, November 19, 2019 9:04 AM
To: Robert Herz
Subject: US v. Schwier: specifications question re: Dkt. 249

Mr. Herz:

Good morning.

In Dkt. 249 at 10, Mr. Fischbach wrote: "Towards that end I am amenable to the government providing to me a computer configured to my specifications. In order to assure scientific results, I have to personally conduct the installation of any software to be tested."

Please promptly advise what "specifications" Mr. Fischbach is requesting.

Thank you,

-Jonas M. Walker
Assistant United States Attorney
District of Alaska
907.271.3983

Robert Herz

From: Robert Herz [rmherz@gci.net]
Sent: Thursday, December 19, 2019 7:25 PM
To: 'Walker, Jonas (USAAK) 5'
Subject: RE: Hardware and software Specifications

Mr. Walker,

The defense will respond *seriatim* to your several factually inaccurate statements in your Dec.7 email.

You wrote: On 11/19/2019, your email (attached) indicated that Mr. Fischbach "believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation."

First, the defense in the Nov.19 email was trying to work cooperatively, and point out that a *possible* option *might* be to use the existing machine on site; hence the use of the conditional phrase that [the existing machine] "may" be able to accommodate TD installation. You ignore the conditional nature of this statement. Moreover, your quote above is taken out of context and ignores the rest of the email which states: "Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, ***Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions.***"

You wrote: Then, on 12/6/2019, your email (attached) indicated that the original computer was inadequate, and requested the government "allow Mr. Fischbach to use the machine that was recently sent to the RCFL."

This part of your email is even more troublesome, as the Dec.6 email has nothing to do with the defense wanting to use the newly provided machine to test TD. The defense request was in reference to not being able to run on the existing machine the VMWare software that Det. Erdely used to run his "validation." The defense was requesting the ability to use the newly provided machine to see if we could run the VMWare software on the new machine so the defense could begin finally to evaluate the data generated by the government "validation." Mr. Fischbach had traveled several hours to the RCFL to begin a review of the government validation. The defense was trying use precious time and resources already committed to being at the RCFL for the day, and the government had already previously instructed Joe Monroe that the defense could not have access to the new machine at all; because the government had apparently just realized that day it had released the TD software into the wild by including it along with the validation that had been sent to the RCFL. This was the second time the government had released sensitive information concerning the TD software without so much as a protective order in place, and again had to depend on the honesty of Mr. Fischbach to maintain security over your software that the government does not seem able to keep secure.

You wrote: Now, however, in your email, below, you are requesting a third computer and identifying additional requirements.

The defense has not requested a "third" computer with "additional requirements." As you well know, the defense did not request the first government supplied machine, a "vintage" out of date Mac that was sent from Anchorage-FBI to the RCFL. That was a machine supplied by the government without any input from the defense. The defense also did not

request the newly provided machine either. That again was supplied by the government *by fiat* even before any specifications had been provided by the defense, in seeming defiance of the court's order at Doc. 254 and Doc 262.

The defense has repeatedly requested the government comply with the court's order that the government supply documentation, software specifications, and installation instructions. The court order at Doc. 262 only relieved the government of supplying a computer by Dec4. Yet, the government sent a computer to the RCFL anyway, and pre-loaded it with software the government used to run its validation. The defense recognizes that it is the government's goal to limit defense testing to only running the government validation. The defense has made clear that it does not intend to run the government "validation" again, as it has no scientific validity.

Other than being relieved of the duty to supply a computer by Dec.4, no other portion of the court's order at Doc. 254 was stayed or vacated. The government is not in compliance with the court's order, as the defense has never received any TD software specifications or installation instructions. The defense, again in an attempt to accommodate the government, save time, and work cooperatively, nevertheless took time to at least analyze the new machine's system specifications by having the RCFL's Joseph Monroe "boot" it up, again after seeking permission from you. The defense did this to see if the new machine sent by the government without any input from the defense could potentially be used to run the defense tests. It was not adequate.

I don't mind a "hard fight," but you seem quite comfortable playing fast and loose with the facts, as exemplified in the above email from you dated Dec7. It's not the first time this has happened in this case. I find it disturbing. In that regard, your "out of office" email response that I received on Dec. 4 says you "may have limited opportunity to read or respond to your email during December 2 - 13, 2019." On Nov.26 at the hearing you did not indicate to the court you would be out of the office from Dec.2 to Dec. 13, presumably on leave, and that's why you could not meet the court's earlier set deadline to respond to the defense motion for reconsideration. Instead you indicated that FBI technical experts needed all that time until December 13 to advise you and respond to the technical issues raised by Mr. Fischbach. Perhaps it's just coincidence that the technical experts needed the same amount of time to respond that coincided with your time out of the office. It would appear that is why you then requested an additional 7 days after your returned to the office to file a response. The coincidence is striking, and I wonder whether the FBI technical experts that were telephonic for that hearing, if they were called to testify, if they would testify that they were the ones who needed more time, as opposed to you. If the real reason for the delay was your vacation, that would represent a serious lack of candor with the court.

Your wrote: In the event that a government-owned computer with Mr. Fischbach's requirements is not available, is the defense offering to provide such a computer, which would remain at the OCRCFL, and which the government and Mr. Fischbach would confirm is "wiped" after the case is complete? If such an arrangement is consistent with the to-be-ordered protective protocols, then that may be best way for the defense to use exactly the computer it wants.

As you learned from your invasive contact with Joseph Monroe regarding the Defense examinations at the RCFL, as well as Mr. Monroe's testimony, the RCFL isn't secure. The Defense has already had equipment stolen or gone missing from the RCFL. While the court has not obligated us to do so, the Defense is not inclined to leave a defense machine worth thousands of dollars there if it cannot be secure and the RCFL will not take responsibility for securing it. Mr. Monroe himself has testified that the RCFL does not have the level of security necessary, and it will not be held accountable for

securing Defense property. It seems questionable if it is even capable of securing the VMWare images, containing TD software that has already been copied to the Defense-privileged Government-owned Mac Tower, currently in the RCFL's civilian workspace, where other civilians sit within inches of the machine, and even utilize some of the same hardware. Even Mr. Monroe himself admitted that the RCFL civilian exam room does not have the level of security of other locations, such as the LA SCIF. Indeed, the court asked the government to address use of the LA SCIF as a location for additional and further defense examinations in this case.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Saturday, December 07, 2019 4:48 PM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Arce, Charisse (USAAK) 1
Subject: RE: Hardware and software Specifications

Mr. Herz:

Good evening.

On 11/19/2019, your email (attached) indicated that Mr. Fischbach "believes that the government-supplied Mac already at the RCFL may be able to accommodate TD installation."

Then, on 12/6/2019, your email (attached) indicated that the original computer was inadequate, and requested the government "allow Mr. Fischbach to use the machine that was recently sent to the RCFL."

Now, however, in your email, below, you are requesting a third computer and identifying additional requirements.

The court has allowed the government to file additional briefing by December 20, 2019, regarding protective protocols. That filing may, also, respond to the latest defense request.

In the event that a government-owned computer with Mr. Fischbach's requirements is not available, is the defense offering to provide such a computer, which would remain at the OCRCFL, and which the government and Mr. Fischbach would confirm is "wiped" after the case is complete? If such an arrangement is consistent with the to-be-ordered protective protocols, then that may be best way for the defense to use exactly the computer it wants.

Thank you, and have a nice weekend,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Friday, December 6, 2019 5:04 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: Hardware and software Specifications

Mr. Walker,

I would agree that Mr. Fischbach is in the best position to know what his needs are in order to conduct defense testing of the TD software. As such, Mr. Fischbach has concluded his inspection of the system requirements of the laptop supplied by the FBI, and it will not be sufficient to meet defense testing needs. It is a 2014 vintage A1398 MacBook Pro, with minimal speed and memory, and outdated hardware and port specifications. Similar to the machine currently in use at the RCFL, it is unlikely that this laptop also will not support running the Virtual Machines supplied by Mr. Erdely. This machine was the least powerful configuration of MacBook Pro produced in 2014. But, is far slower than the minimum requirements of today's Macs. Notably, at this juncture the Government is seeking an order that Mr. Fischbach only use an Ethernet port. This machine does not have an Ethernet port.

The following are the *minimum requirements* needed in a government supplied machine necessary to conduct defense testing of the TD software. Defense specifications are in black, corresponding specifications of the computer supplied by the government are in red:

2.6GHz 6-core 9th-generation Intel Core i7 processor (4-core 4th generation processor discontinued in 2015 nearly five years ago)

64GB 2666MHz DDR4 memory (16GB 1600 MHz DDR3 -- incapable of additional RAM)

AMD Radeon Pro 5500M with 8GB of GDDR6 memory (2GB discontinued graphics processor)

512GB SSD storage (Unknown)

Thunderbolt / USB-C (No USB-C)

WiFi & RJ45 Ethernet (No Ethernet)

The Mac laptop also must have Bootcamp & **valid** Windows 10 installed.

Please let me know when a machine with these minimum requirements will be supplied and available for Mr. Fischbach's use.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Friday, December 06, 2019 3:31 PM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Arce, Charisse (USAAK) 1; Russo, Frank (USAAK); Allison, Daryl (AN) (FBI)
Subject: RE: Hardware and software Specifications

Mr. Herz:

Thank you for contacting me regarding you concerns.

Per my email of 12/4 below, the government believes that the computer provided is sufficient to run TD as it would be used in an investigation.

The government does not know what tests Mr. Fischbach intends to run, as the defense has withheld that information from the government. Without knowing what tests Mr. Fischbach intends to run, and the technical requirements of those tests, the government is not in a position to opine regarding what technical specifications are necessary to meet Mr. Fischbach's needs.

Because Mr. Fischbach has access to the technical specifications of the computer, as described below, Mr. Fischbach is the person best situated to answer your question regarding whether the computer is sufficient to run Mr. Fischbach's tests.

Thank you,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Friday, December 6, 2019 2:56 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: Hardware and software Specifications

Mr. Walker,

I agree the court stayed the requirement that the government does not need to provide the TD computer. But the court did not stay the entire order at Doc. 254. As such, the requirement that the government provide all software documentation related to TD is still binding on the government.

Moreover, I believe this was in recognition that the defense needs the TD software specifications in order to provide a tailored request for computer specifications for the computer that the defense needs to runs its tests. Nevertheless, the government prior to knowing what the defense specifications would be, "selected" a computer that the *government believes* the defense should use. This was not the process the court envisioned by its order at Doc.254 and seems a bit "cart before the horse." Given that Doc.254 was not stayed in its entirety, I disagree that the government has complied

with the court's orders, or that the court's orders have been exceeded. That Mr. Fischbach is attempting to ascertain the system requirements of the computer the government provided, prior to defense input, only means we are evaluating what has been sent to see if it will meet defense needs. Our preliminary review suggests that it will not be adequate. When Mr. Fischbach completes his work at the RCFL later today, I will provide the government notice of what specifications are, in fact, needed, and whether the computer sent prematurely will meet defense needs. However, the lack of TD software specifications has significantly hampered the defense in this evaluation.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Thursday, December 05, 2019 5:44 AM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Monroe, Joseph; Allison, Daryl (AN) (FBI); Steeves, Holly J. (AN) (FBI); Arce, Charisse (USAAK) 1
Subject: RE: Hardware and software Specifications

Mr. Herz:

Good morning. I replied in a separate email chain regarding the defense request for Mr. Monroe to show Mr. Fischbach the computer settings. As indicated, I don't object to that request, and I appreciate Mr. Fischbach's suggestion that he see the settings in person to get the data he needs. That seems like an efficient way to get the data directly to Mr. Fischbach.

At Dkt. 262, the court vacated the order at Dkt. 254 in that the government does not have to provide the TD computer to Mr. Fischbach at this time.

Also in Dkt. 262, the court ordered the defense to provide specifications by 12/6. To assist the defense in this process, I provided the specifications of the selected computer in a prior email chain yesterday; see below, immediately prior to your email.

Accordingly, the government has complied with the Court's orders, and, in fact, has exceeded them, in that Mr. Monroe will be showing the computer details to Mr. Fischbach, which is what Mr. Fischbach requested.

The Court will, no doubt, appreciate the parties' cooperation regarding these technical details.

Thank you,

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Wednesday, December 4, 2019 2:49 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: RE: Hardware and software Specifications

Mr. Walker,

Unfortunately, this is insufficient information to allow the defense to make a determination whether this machine will be adequate for defense testing purposes. Will you allow Joe Monroe to boot up the computer on Friday in Mr. Fischbach's presence so that more specific information can be obtained about what has been sent?

In addition, does the government intend to provide more and complete information regarding TD software specifications before this Friday, and as required by the court's order at Doc.254?

Thank you for your attention to these requests.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Wednesday, December 04, 2019 12:41 PM
To: Robert Herz
Cc: 'Jeff M. Fischbach, ABFE'; Allison, Daryl (AN) (FBI)
Subject: RE: Hardware and software Specifications

Mr. Herz:

I am advised that a computer with the following characteristics has been identified, which the government expects to be sufficient:

Apple MacPro laptop with Windows 10 Pro loaded on Bootcamp partition Laptop has 16GB of RAM, 64-bit Operating System x64 based processor with a 250GB Hard Drive

Thank you;

-AUSA Jonas M. Walker
907.271.3983

From: Robert Herz <rmherz@gci.net>
Sent: Tuesday, December 3, 2019 11:41 AM

To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Cc: 'Jeff M. Fischbach, ABFE' <jeff@secondwave.com>
Subject: Hardware and software Specifications

Mr. Walker,

At Doc. 262 the court ordered the defense to provide the government with the computer specifications the defense deems necessary to allow defense testing of the TD Software on a computer the government will provide for defense testing. Based on information provided to the government in email correspondence, pleadings, and declarations, the defense has made it clear that hardware specifications are predicated in part on the software the computer will run, meaning that it is important to know the specifications of the TD software. Ultimately, defense computer hardware specifications will be based on TD specifications as well as the various software Mr. Fischbach will install and that are needed for defense testing. The court ordered the government at Doc. 254 to provide the defense "with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements." To date, the government has provided only a user manual for TD version 1.23, and it was redacted. This does not comply with the court order, and prevents the defense from more meaningfully providing computer specifications to the government by this Friday. The defense has provided the government with specifications recently in Mr. Fischbach's declaration at Doc. 261 para.8. The defense believes that the court intends for the parties to refine these specifications which is why the court changed the defense deadline to December 6. If the parties are to refine the specifications as the court intends, then the government must provide TD software specifications as directed in the court's order at 254, which in turn will allow the defense to make a more refined and tailored request concerning computer specifications. If the government is not willing to fully disclose software specifications to both TD versions in a timely manner and *before* Friday, which is necessary to allow for defense review and evaluation, then the defense will be unable to refine the specifications previously provided to the government, and those previously provided specifications will stand as to what the defense will be requesting.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

Robert Herz

From: Walker, Jonas (USAAK) 5 [Jonas.Walker@usdoj.gov]
Sent: Friday, December 06, 2019 3:25 PM
To: Robert Herz
Cc: Monroe, Joseph; Russo, Frank (USAAK); Allison, Daryl (AN) (FBI)
Subject: RE: Schwier: Confirming that virtual machine will not be copied

Mr. Herz:

I appreciate the quick response. My understanding is that Mr. Fischbach is requesting access to the Apple MacPro laptop.

Before I respond, I will request that Mr. Monroe confirm that TD software is not currently loaded onto the Apple MacPro Laptop.

Mr. Monroe: Can you please review the Apple MacPro Laptop and confirm that TD is not currently loaded onto it?

Thank you,

-AUSA Jonas M. Walker
907.271.3983

-----Original Message-----
From: Robert Herz <rmherz@gci.net>
Sent: Friday, December 6, 2019 2:31 PM
To: Walker, Jonas (USAAK) 5 <JWalker5@usa.doj.gov>
Subject: FW: Schwier: Confirming that virtual machine will not be copied

More accurately, I should say, that the machine from Anchorage DOJ will not open the VMs using the VMware software that Mr. Erdely used to create the VMs, i.e. the machine will not run the VMware software.

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

-----Original Message-----
From: Robert Herz [mailto:rmherz@gci.net]
Sent: Friday, December 06, 2019 2:11 PM
To: 'Walker, Jonas (USAAK) 5'
Cc: 'Jeff M. Fischbach, ABFE'
Subject: RE: Schwier: Confirming that virtual machine will not be copied

Confirmed.

In full disclosure, prior to knowing that TD may be on the VMs Mr. Fischbach in the presence of Mr. Monroe had copied the flash drive contents onto the computer previously sent to the RCFL from DOJ-Anchorage/FBI-Anchorage.

However, in speaking with Mr. Fischbach, the computer sent from Anchorage that Mr. Fischbach has been using does not have system requirements sufficient to open the flash drive containing the packet capture data or the VMs. Will you allow Mr. Fischbach to use the machine that was recently sent to the RCFL?

Robert M. Herz
Law Offices of Robert Herz, P.C.
The Seventh and E Building
431 West Seventh Avenue, Suite 107
Anchorage, Alaska 99501
Tel. 907-277-7171
Email: rmherz@gci.net
Website: www.robertherzlaw.com

-----Original Message-----
From: Walker, Jonas (USAAK) 5 [mailto:Jonas.Walker@usdoj.gov]
Sent: Friday, December 06, 2019 1:37 PM
To: Robert Herz
Cc: Robert Erdely; Allison, Daryl (AN) (FBI); Arce, Charisse (USAAK) 1; jeff@secondwave.com; Joseph Monroe; Russo, Frank (USAAK); Cook, Brian J. (WF) (FBI)
Subject: Schwier: Confirming that virtual machine will not be copied

All:

Per email traffic, Mr. Fischbach is accessing a flash drive containing packet capture data and virtual machines (VM) from the validation testing that occurred with Det. Erdely in Anchorage. The VMs may contain TD software.

It is the government's understanding that Mr. Fischbach will not be copying the VMs onto his own media (computer, flash drive, etc) or in any way removing the VMs from the OCRCFL.

Mr. Herz, please reply in writing to confirm this correct.

Thank you,

-Jonas Walker
AUSA, District of Alaska

Sent from my iPhone

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Ph. / 907-277-0281 Fx.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

RESPONSE IN OPPOSITION TO GOVERNMENT CONSOLIDATED FILING AT DOC. 288

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. hereby files this response in opposition to the government's multiple pleadings consolidated as filed by the government at Doc. 288. The government has filed 1) a status report; 2) a notice regarding proposed testing environment; 3) a response to the defense motion for reconsideration at Doc. 256; and 4) an responses in opposition (styled as "responses to objections") to the use of the SCIF located at the Los Angeles federal court and to defense computer specifications. All these pleadings were contained in one document.[1] The court invited the defense at Doc. 289 to file a response to the government's filing. Mr. Schwier will respond *seriatim*.

1) Government's Status Report. The government filed a fourth superseding indictment on December 18, 2019, over two years and four months since the government first indicted Mr. Schwier. This iteration of the indictment, as alleged in count 4, for the first time alleges conduct

[1] This consolidated filing seemingly violates local court rules. See, Local Crim Rule 1.1(b); Local Civ.Rule 7.1(e) and 5.1(f)(2) which require separate pleadings be filed for separate issues.

of *receiving* images pertaining to the date of *November, 2015*. No previous iteration of any indictment in this case alleges conduct from the year 2015. The government offers no explanation for this delay. The government gave notice to the defense on December 27, 2019 that four images that the government intends to rely upon were available to review at the RCFL. After receiving that notice, that same day the defense requested the government provide the filename, pathname, MAC data, and hash values for each image prior to Mr. Fischbach before making the trip to the RCFL. The images themselves are of little value in the context of conducting a forensic computer examination. Today, the government responded to the request but did not provide filenames, pathnames, MAC data and hash values as requested. See Email Chain attached.

2) Government Notice of Proposed Testing Environment.

The government has seemingly repudiated the testing protocol as provided for in the Court's orders at 231, 243 and 254 the terms of which the government previously has approved. The government has twice proposed additional terms to the protective order. See, Doc. 244-1 and 253-5., which have largely been adopted by the court. The only objection raised by the government to the court's protocol, as indicated in its Motion for Reconsideration at Doc.255, was that the court did not mandate any packet capture software. Id. at Doc.255, page 2. The only remaining issues to be resolved were the ones raised by Mr. Schwier at Doc. 256 in his Motion for Reconsideration.

Contrary to the government's claim, the court did not order the government to submit a revised protective order protocol.[2] The court only invited the government to respond to the objections raised by the defense its Motion for Reconsideration at Doc. 256. Purportedly, the government needed to consult with FBI technical experts before it could offer a response to the technical issues raised by the defense. Instead, the government has filed a whole new

[2] The government alleges that "At the hearing on November 26, 2019, the Court ordered the government to submit a revised protective protocol." Govt. Doc 288 at 2. Mr. Schwier does not believe the hearing record supports this claim and certainly nothing in the court's order at Doc.262 does.

protocol proposal that is regressive nature, and makes defense testing impossible,[3] as detailed by Mr. Fischbach in the attached Declaration. This new testing protocol creates serious obstacles to defense testing including but not limited to the lack of internet access, dictating a testing environment, government monitoring of defense testing in real time, and prohibiting use of defense equipment and software, among others. Comparing the Government's prior proposal at Doc. 253-4 to its new proposed protocol at 288 and 288-1 should be instructive.

a) Internet Access

Det. Erdeley has made clear that Internet access is required to run and test Torrential Downpour ("TD") software. This was acknowledged by the government: "The defense may bring... an internet hotspot (i.e. one that is compatible to connect to the TD Computer via the network card) into the OCRCFL room with the TD Computer. Doc. 253-4, para. 6. Whereas now:

> "Internet access will be **provided by the government for the limited purpose of installing uTorrent** software or other software that requires activation/installation via the Internet on one or more of the test computers. All of the Internet installations/activations/ connections will be conducted prior to the installation of TD. **Once the installation of defense's software is complete, the Internet access will be terminated** for the remainder of the testing period."

Doc. 288-1 at para. 5. Emphasis supplied. Previously the government required the defense to bring its own private wireless Internet hotspot, for testing purposes. The Defense is now required to use a **government monitored** Internet connection, but only to install the software that Mr. Erdely used. Following that, the defense has **no Internet for testing purposes,** as required by TD, and in compliance with previously stated defense test specifications determined to be material by the court. Instead of privileged defense methodology and testing, the government will now have monitored access to test results before counsel does.

[3] The defense infers that once the Office of General Counsel for the FBI and the FBI technical experts saw the extant terms of the protective order and testing protocol, they strenuously objected and hence proposed entirely new and more regressive terms that they wish to impose upon and govern what should otherwise be independent defense testing in this case.

b) Use Of Defense Testing Equipment

The government previously agreed that: "the defense may bring digital media, computers, cell phones" into RCFL exam room for defense testing purposes. Doc. 253-4 at Para. 6. However, now the government has completely retreated from this position and states:

> **No other electronic devices** or storage devices may be brought into the testing room to include but not limited to **computers, phones, laptops, hard drives, or tablets.**

Doc. 288-1 at para. 3. If the court were to adopt this provision, it would mean that the defense has no means of using any hardware necessary to complete its testing, nor any industry standard hardware necessary to insure that no software or data is unintentionally copied, nor the ability for the defense expert to even communicate with counsel during tests.

c) Use Of Defense Testing Software

Previously, the government agreed that: "prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer, all while in the physical presence of the FBI agent or Task Force Officer. The FBI agent or Task Force Officer may observe Mr. Fischbach install the software. Doc 253-4. at para. 5b.

> **All software** installed on testing computers cannot be encrypted or password protected and **will be copied/hashed/preserved/ sealed.** The copies will be preserved and only accessed by the government upon Court authorization. (Doc. 288-1 at para 1).
>
> Before defense may install any software on the testing computers the government will conduct virus scans on the software in the presence of the defense expert. (Doc. 288-1 at para. 2) ***
>
> This installation of defense's software will be done in a user account designated for Defense. Government will provide access to the Defense user account for this installation process.

Doc. 288-1 at para 11. Prior defense concerns were that an agent could discern privileged methodology by observing defense software installation. The current government proposal requires the defense to provide licensed and/or proprietary software to the government. The

defense has no authority to grant licenses to the government. The government has not addressed concerns about the government *observing* the defense software installation and instead now is requiring the defense to provide the information to the government. Virus scans only serve to provide *more* information about defense methodology. They do not serve to protect government computers, as the government should have *no access* to this equipment in the first place. Under the government proposal, defense software cannot access TD, yet the government is demanding access to examine defense software, which -- under the government proposal -- cannot even directly access TD software. The defense testing methodology cannot work without direct access to TD, using defense software.

d) Wireshark Monitoring

Previously the government sought an Order from the court requiring the defense to use a packet capture technology. The defense objected, and the court did not require that it be used.[4] The government in Doc. 253-4 proposed: "All communications with the TD Computer will be preserved via Wireshark. This preservation includes all communications with TD during testing, and at all times the computer is powered up. The defense shall maintain the Wireshark data pending further order of the Court. Doc. 253-4 at para. 13. Now the government proposes an even more onerous and invasive use of Wireshark:

> **One laptop will be dedicated to capturing Wireshark files** for the entire testing period. At the conclusion of the testing, **defense expert may witness the government storing these files** on a CD, hashing them, and sealing them for preservation. The government will not access these files unless the Court authorizes government access. Doc. 288-1 at para 6.
>
> Laptop 4 – **Defense will not be provided any access to this computer**. Wireshark files will be stored here during the testing period.

[4] The government sought reconsideration of this issue in Doc. 255 but agreed at the hearing on November 26, 2019 that it was moot based on the information contained in the filing by the defense at Doc. 256 and Mr. Fischbach's contemporaneous declaration. The defense acknowledges that the court has warned the defense in writing and orally that failure by the defense to use any packet capture software could potentially render some of Mr. Fischbach's testimony inadmissible under *Daubert*.

Doc. 288-1 at para. 9.

Prior defense concerns were that the government was requiring the defense to create and preserve discovery for the government. Now the government is requiring *real-time* access to that discovery which will be held and preserved *by* the government. The government has proposed that a switch/router will be operating in their test environment system, and that the defense will not have access to it, which means only the government will have access. Anyone from the government would be able to and can plug a computer into that router and monitor in real time what the defense is doing. And in fact that is exactly what laptop 4, the proposed Wireshark computer, will be doing. The defense will not have access to Laptop 4 either. Anyone from the government would be able to and can observe the screen/monitor of Laptop 4 in real time to see what the defense is doing. Moreover, as described by Mr. Fischbach the Wireshark log files and defense results can be manipulated by the government before the defense would be able to see their own results The defense, in this case, will not even have access to their own discovery, as noted in 288-1 at para 9.

e) Testing Results

Previously the government agreed that the "The defense may bring digital media..." into the exam room at the RCFL. 253-4 at para. 6. Now the government has completely repudiated this:

> Defense testing may generate files that are stored on the host computer of Laptop 1, and/or Laptops 2 and 3. Upon conclusion of testing, all files will be copied/ hashed/preserved/sealed and only accessed by the government upon Court authorization. Doc. 288-1 at para. 4.
>
> If requested by the defense expert, at the conclusion of testing **the government will make a copy of the files generated by the defense** software which were stored on Laptop 1, 2, and/or 3. This copy will be on a CD, which will be hashed and **will remain at the OCRCFL** to be available for the defense expert to come and conduct further analysis. If requested by defense, then this CD can be sealed and marked by the defense expert. The CD will not leave the OCRFL.

Doc 288-1 at para 11, 14. A prior concern was that while defense media could be brought into the exam room at the RCFL, the government sought to block the ports which prevented the defense from being able to remove defense results to Mr. Fischbach's office for further analysis. This new proposal still blocks the ports, but now also requires results to be provided to the government. The results themselves would not contain contraband and would not contain a copy of TD, and so attempting to restrict Mr. Fischbach from being able to analyze results using his own equipment and software at his office does nothing to protect TD from being released to the general public and only serves to make defense testing unnecessarily inconvenient and expensive. Under these requirements, the defense will have no ability to further analyze its own test results, while the government must be trusted not to access privileged defense work product. Furthermore, the defense cannot even bring in the hardware necessary to conduct the primary testing that the court has already determined to be material, let alone use hardware necessary to analyze its own results in a non-government environment.

f) Real-Time monitoring of Privileged Defense Work Product

Previously, nothing in any government proposal allowed the government to monitor any part of defense testing, including test design, methodology, use of software or hardware, or communications. Now the government proposes that it be allowed to have the capability to engage in real-time monitoring of defense testing, as previously noted and referenced in Doc. 288-1 paragraphs 6 and 9.

3) Reply to Government Response in Opposition to Defense Motion for Reconsideration

In its Motion for Reconsideration at Doc. 256 the defense noted that paragraph 9 of the court's order at Doc. 254 limited the defense to the use of one port. The defense noted that:

> this restriction prevents [Mr. Fischbach] from installing industry accepted software and hardware as well as prevents him from removing his test results from the government provided computer for further examination and analysis on his own equipment, and/or in his own forensic work environment. He would be unable to

> connect a screen, keyboard, or mouse, let alone the hardware and software that he needs for his tests. Doc.. 256 at 2.

The government's only response is that under the government designed testing environment Mr. Fischbach would be able to use a screen, a mouse and a keyboard, and therefore the objection has no merit or is moot. Doc. 288 at 3. The government fails to respond to the main point of the objection raised by the defense: limited port access prevents Mr. Fischbach from installing his own testing software and hardware and from being able to remove results for further examination and analysis in his own forensic work environment.

Next, the government attempts to respond to the defense objections to paragraphs 6 and 7 of the court's order at Doc. 254. The defense argued that the terms of Paragraphs 6 and 7 of the court's order compromise attorney-client privilege and attorney work product by intruding upon the confidential and independent defense testing process. The government's response is nonsensical. The government asserts that the defense has no work-product privilege associated with TD. The defense has never asserted that it did. What is clear, though, is that the work of agents for the attorney in preparation of litigation is protected by the work product doctrine. United States v. Richey, 632 F.3d 559, 567 (9th Cir. 2011). The defense has asserted that the design of the defense testing environment, how equipment is configured, what software and hardware is used, which tests are run, what data is examined would all reveal information that is privileged at this point. The privilege would only be waived *if* Mr. Fischbach were to testify about this subject at trial. The government fails to meaningfully respond to this issue.

The defense has never argued that the mere presence of the computer with government installed contraband and government installed software located at the OCRCFL is in any way privileged. The defense has not argued that Mr. Fischbach's communications with Mr. Monroe are privileged, only that in Mr. Fischbach's experience the government's intrusion into these communications seems to violate long standing nationwide RCFL policies to

maintain the sanctity of independent defense testing of contraband that must occur in a government facility. None of the emails written by Mr. Fischbach to the government or Mr. Monroe divulged anything pertaining to the design of the defense testing environment, how equipment is configured, what software and hardware is used, which tests are run, and what data is examined. None of the emails filed by the defense in this case waived any of this privileged information.

Mr. Fischbach does, indeed utilize industry standard hardware, software, and procedures. As well, over the course of 25 years, Mr. Fischbach has developed and engineered some of his own, many of which have been taught to and utilized by others in the field. There are, however, numerous industry standard forensic practices, software, hardware, and procedures from which a forensic analyst may choose to conduct an examination, based on their appropriateness to the allegations and evidence in question. By way of example, any professional sport has rules and acceptable conduct. The mere fact that opposing teams are required to play from the same rulebook, and will likely choose from a limited number of viable playing strategies, does not negate the fact that *any* strategy would be thwarted if the opposing team were allowed to observe team meetings prior to taking the field.

4) Use of a more secure testing environment: the SCIF or FBI-Wilshire.

The government objects to moving the location of the defense testing in this case to a more secure location. The government has repeatedly asserted that its overriding concern is for the prevention of the release of TD into "the wild," since any release would compromise on-going and future investigations. The exam room at the OCRCFL is open to various defense experts and attorneys working on different cases. A piece of Mr. Fischbach's own equipment disappeared from this room. Mr. Monroe acknowledged that the RCFL was not as secure as the SCIF or the FBI offices at Wilshire. The defense proposed each of these two alternative locations as more secure environments for testing the government's sensitive

software. Under the circumstances, it would seem the government would want to utilize a more secure location for testing of the TD software in order to protect it.

The government observes that this case does not involve classified information. This is true. And while the government suggests for this reason alone the request to use the SCIF is unusual, the government does not claim, as it cannot, that this prevents use of the SCIF in this case. "Unusualness" or "appropriateness" should not be the government's overriding concern considering the government's self-imposed "level of security" that it has imparted to its software. Thus far, the elements which the government maintains must be kept secret it, the government has already exposed to the defense. Given that both parties, as well as the OCRCFL's own Joseph Monroe, agree that RCFL facilities are not equipped to monitor against theft of hardware and software, out of an abundance of caution, the defense has simply attempted to provide secure alternatives, based on Mr. Fischbach's established experience with more secure government facilities.

While Mr. Fischbach acknowledged on record that he has not had the need to renew his National Security Status, if necessary in order to analyze the TD software in a secure environment, he would be willing to undergo an expedited review, as he did in the U*.S. v. Chi Mak* case cited by the government. Furthermore, he notes that in his experience, the SCIF in Los Angeles simply consists of isolated single rooms, containing no access to sensitive information, *other than that which the analyst is currently examining.* Thus, while this may be a "inconsistent use" -case, the treatment of software as "government sensitive" is also an "inconsistent use"-case when compared with all other standard investigative software which have been openly tested and utilized by the forensic community.

Lastly, the defense notes that the government has not raised any objection to moving the testing location to the FBI-Wilshire office. This would be a more secure location than the RCFL and could be used for both testing of the TD software as well as for continuing evidence review.

5) Government provided computer specifications are insufficient.[5]

The government erroneously asserts that the defense specifications for a government supplied computer have been "evolving." The government continues to refer to an email dated November 19, 2019 as somehow constituting a hardware specifications request from the defense. The government continues to conflate the facts, as pointed out in the email thread at Doc. 281-2.[6] As the defense pointed to the government out then: "Due to the lack of production of any TD documentation, manuals, information pertaining to operating requirements, or any other materials, ***Mr. Fischbach is only able to render an educated guess as to the ability of the equipment at the RCFL to accommodate both TD versions.***" That cannot reasonably be construed as a hardware specification request.

What has made the "project more difficult" has been the government's unwillingness to provide the software specifications, installation instructions, and user manuals as ordered by the court so that the defense could make a tailored defense specifications request. Given the government failure to be forthcoming about TD software specifications, the government should not be heard to complain now that the specifications ultimately provided by the defense are not to their liking.[7]

---

[5] Again, the government asserts that the court ordered the government to respond to defense objections to a government provided computer. The record does not support this assertion. The defense had not made objections to any government supplied computer prior to the November 26 hearing. The court at Doc. 254 ordered the government first to provide to the defense TD software specifications and then the defense was required to provide its computer hardware specifications needed to run its defense tests. Only if the defense did not provide these specifications in a timely manner did the court permit the government to supply equipment that the government thought was "reasonable" under the circumstances.

[6] See, Email Chain at 281-2, specifically dated December 19, 2019 addressed to AUSA Walker.

[7] It is not accurate to describe the defense proposed computer as "state of the art or "top of the line" indeed the proposed specifications are for a mid-range quality computer, albeit "new in box" as the defense has no way of knowing what kind of used computers are in government inventory at any given time.

The government assumes defense testing is attempting to simulate actual investigative activity[8], in part to justify its own test design (which they call the "testing environment") and to justify the computers it has chosen. However, the government admits it knows nothing about the tests the defense will run, or the software the defense plans to use, so it is presumptuous to assume that spreading out functions over three computers is a test design that the defense will utilize or that the specifications of the computers the government has chosen will be sufficient for defense tests that are entirely different from and whose purposes are different from anything the government has heretofore done. It may be true that TD can operate on less powerful computers, but this is not relevant as this fails to account for the defense hardware and other software that the defense will use for defense testing that requires more computing power than that needed for simply running TD software.

The proposed specifications of the computers the government wants to supply are inadequate because, Mr. Fischbach is not simply *operating* TD, he is testing it. Thus, the operating specifications the defense has requested from the government,[9] are simply a baseline in order to properly specify hardware and virtual machine variables. While the government continuously specifies environments only suited to approximate Mr. Erdely's validation procedures (minus the required Internet accesses). The defense, however, has outlined specific tests of the TD software which require other hardware and software to complete, demonstrate, and reproduce the defense tests. In addition to that, *both* the government and the defense have

---

[8] The government writes: "During the actual investigation of Mr. Schwier the Torrential Downpour software was on a different computer than Mr. Schwier's computer, and, therefore, keeping those functions on separate computers more closely simulates the actual investigative activity." Doc. 288 at 11.

[9] Despite the government's claims to the contrary, the defense is unable to locate in the TD materials provided by the government anything that would be considered "software specifications." On page 7 of the User Manual there is a paragraph titled "System Requirements." Its only content consists of two lines: *"Torrential Downpour runs on Windows Vista or later, and requires Microsoft.NET 4.0 or later. You also need sufficient disk space to hold the files that you download."* The government's claim that it provided software specifications seems disingenuous at best.

specified the need to use multiple "Virtual Machines (VMs)." Mr. Fischbach has already tested the use of just a single Virtual Machine on equipment with specifications equivalent to those proposed, and on the machines provided by the government, and it was entirely non-functional. Thus, the government's proposed hardware simply cannot be used, even for the government's own Validation.

DATED at Anchorage, Alaska, this 6th day of January 2020.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
Phone 907-277-7171
Fax 907-277-0281
rmherz@gci.net
AK Bar No. 8706023

CERTIFICATE OF SERVICE
I hereby certify that on Jan 20, 2020, a copy of the foregoing Notice of Compliance with Order at 262 was served electronically on Assistant United States Attorney's Office s/ Robert Herz

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America, Plaintiff, vs. Matthew Schwier, Defendant.	Case No. 3:17-cr-0095 SLG-DMS

DECLARATION OF JEFFREY M. FISCHBACH

I, Jeffrey M. Fischbach, declare as follows:

1. This declaration is written in response to the government's Dkt. 288, "Notice Regarding Proposed Testing Environment", and 288-1, "Test Environment Regarding Torrential Downpour".

2. In both writing my November 25, 2019 Declaration, and at the hearing on November 26, 2019, I attempted to articulate compromise, in order to assuage the government's concerns for its proprietary software; while remaining focused on the tests deemed necessary in order to competently prepare counsel for trial. At the same time, I have attempted to observe and

maintain sound scientific and forensic practices -- both necessary to survive a Daubert-Frye challenge, as well as to assure the integrity of my results and to ensure the security of my work product and of the software in question.

3. It appears that the government has almost wholly superseded its Dkt 253-4 with new, much more harsh restrictions proposed in Dkt 288 and 288-1. Nearly every item proposed in Dkt. 288 and 288-1 serves to add additional impediments to Torrential Downpour (TD) testing of any kind, adds several new means for the government to monitor and surveil defense testing, *in real-time*, exposing work product and privilege in the testing process. Yet, while this new proposal adds numerous barriers to performing the tests that the court found material, it does nothing to prevent TD from "escaping" into the "wild".

4. While the defense has objected to being forced to create discovery of its own testing procedures; in Dkt 288 and 288-1, the government has now gone much further than its proposal in Dkt 253-4. As an expert for decades, I understand that my results will be subject to scrutiny-- if used at trial. Hence, I understand I will have to document my work, as well as the forensic measures I have taken to protect assets, such that it could be independently reproduced. The means of doing so, however, has never been dictated to me by the government or by the court.

5. Confirmation bias has long plagued forensics. But, in this particular circumstance, the capability to narrow recorded results by using Wireshark's built-in filters was actually demonstrated by Mr. Erdely during his "validation" sessions. Thus, with the government documenting my work, not only do they see my test results before I can even report them to counsel, but I have no ability to audit my own discovery for accuracy. I testified on November 26, 2019 that Dkt 253-4's proposal that I must maintain a Wireshark log of all my work could be easily manipulated. As a result, it seems, the government has now proposed in Dkt 288-1 that *it* must be able to record and maintain easily-manipulated Wireshark logs of all of my testing, as well as control the router which carries all of my testing traffic. Which, in addition to *very* realistically altering my results before I read them, or for the government to collect conflicting results, it also gives the government the opportunity to filter, intercept and modify every piece test input data from one machine, before it even reaches the other, or to return

modified results. Submitting to this proposal has the making of a forensic science scandal rivaling any of the recent FBI lab scandals. Again, I refuse to be a party to bad scientific practices and dangerous precedent.

6. Dkt 288 and 288-1 does, however, carefully dictate the way that the defense can conduct its tests by not only providing an environment designed around Mr. Erdely's TD "validation", but then completely denying the defense use of the Internet for its testing. Something which Mr. Erdely himself stated, during his validation, was a *requirement* for using TD in any way.

7. Despite the government's failure to secure its own software and secrets, I have gone to great lengths, both to voluntarily alert the government and the court about information which they accidentally provided to me, as well as to attempt to use equipment owned by the government, at facilities run by the government, and to utilize very expensive specialized hardware and software at my disposal to further reduce the risk of accidental dissemination. To wit, I suggested the use of the LA SCIF, when it was demonstrated to me that the OCRCFL does not physically guarantee the security of equipment and data left in its shared defense exam room.

8. In Dkt 288, p7 the government refers to my suggestion to use the Roybal SCIF as "unusual" -- not untenable. All parties seem to agree that RCFL facilities are not equipped to monitor against theft of hardware and software, as has already occurred in this case. Out of an abundance of caution, based on decades of experience with government examination facilities, I have provided objectively more secure alternatives to the OCRCFL. In my experience, the SCIF in Los Angeles are simply isolated single rooms, containing no access to sensitive information, *other than that which the analyst is currently examining.* Thus, while this may be a "inconsistent" use-case, the treatment of software as "government sensitive" is also inconsistent with all standard investigative software, which have been openly tested and utilized by the forensic community. I have had access to the SCIF in Los Angeles, where I had permitted use of my own laptop and cellular devices, with only the admonishment of a "lifelong obligation to protect from disclosure the classified information" to which I had access.

9. The government refers to "*general"* principles of SCIF operation. Thus, one can assume

that these principles apply generally, but not exclusively. And, that while my suggestion for a more secure location to conduct my TD tests is "unusual", it apparently does not go against any particular rules or policies. It should be further noted that, in my *proven* classified experience, while information relative to a particular case is stored in a particular locked and secured SCIF room, the SCIF itself does not provide information to any classified or other case information, beyond the immediate case being examined.

10. I see no reason provided in Dkt 288 to explain why the LA SCIF cannot be used, nor why it is any less secure than the OCRCFL. While the government is correct that the LA SCIF at Roybal is several hours closer to me, which will allow me to complete my work significantly faster, security is the primary reason I suggested this facility, as well as the LA FBI building at Wilshire. I suggested both of these locations before the government decided to impose use of OCRCFL. I have used all three locations in Federal trials many times, and have been long aware that the RCFL does not provide security comparable to the other two sites. Thus, when requesting the ability to continue examining the case in Los Angeles in order to expedite trial readiness, I suggested either the LA Wilshire FBI defense examination facilities or the Roybal SCIF -- for the purposes of hardware, software and data security as well as location.

11. Dkt 288 and 288-1 provide conflicting information, by arguing *both* that I can't use the SCIF because I need to use the Internet and some of my own hardware to conduct my tests, *and* that I can no longer use the Internet *or* my own hardware at the RCFL. While Dkt 288-1, paragraph 3 proposes, "No other electronic devices or storage devices may be brought into the testing room to include but not limited to computers, phones, laptops, hard drives, or tablets", Dkt 288 (Page 8) states, "...the evidence review includes use of the internet and the presence of Mr. Fischbach's computers. Therefore, the SCIF is not an appropriate place for evidence review in this case." It appears here that the government acknowledges the need for the defense to utilize its own equipment and Internet service to complete its testing, for the purposes of denying use of the SCIF, yet denies defense use of its own equipment and Internet service for the purposes of using the less-secure defense examination room at the OCRCFL.

12. Similarly, while Dkt 253-4 (Para 6) specifies exactly what kind of Internet device I may

bring to conduct my tests, Dkt 288-1 (Para 5) completely denies *any* use of the Internet at all for testing. And, while Mr. Erdely has gone on-record that TD *requires* use of the Internet for the "validation" he performed in my presence on November 4, 2019, or use of any Torrent activity, the government has, in Dkt 288-1, once again proposed an environment that appears nearly identical to Mr. Erdely's "validation" methodology. Dkt 288-1 doesn't even allow me to conduct Mr. Erdely's own "validation" procedures, let alone the tests the court has already ruled material.

13. Preventing data from being disseminated is one of the key roles of the established forensic hardware I use in my testing and examination. In this new proposal, while the government suggests that its interests are in protecting the software that *they* have already accidentally released to me *without* any of their proposals in place -- I have now been completely restricted from using any equipment to secure any subsequent copies.

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on December ???, 2019.

Jeffrey M. Fischbach

Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America, Plaintiff, vs. Matthew Schwier, Defendant.	Case No. 3:17-cr-0095 SLG-DMS

SUPPLEMENTAL DECLARATION OF JEFFREY M. FISCHBACH
SUPPLEMENTING DOC. 296

I, Jeffrey M. Fischbach, declare as follows:

1. This declaration is written to supplement my declaration at Dkt. 296-1 responding to the government's Dktt 288, "Notice Regarding Proposed Testing Environment", and 288-1, "Test Environment Regarding Torrential Downpour".

2. It should be noted that the government's entire concern over TD, as well as TD's secret feature being released into the "wild" has been rendered entirely without merit and perhaps disingenuous by its own repeated missteps. As noted previously, the government already

accidentally exposed its secret feature to me during its demonstration on October 17 and 18, 2019. Without prompting or obligation, *I* alerted *both* the government and the court that this occurred, and volunteered to bound by a verbal nondisclosure agreement, sworn before the court. Had I not volunteered this information, the government would have had no idea that this secret, which the government has described as being critical to its ability to work undercover, without detection, had been exposed to me. I have been trusted since then to observe the oath I *volunteered* to the court. The government has now, once again, accidentally provided me something it claims I cannot be trusted to keep safe. Before settling on a protective order, the government has unintentionally provided me with two working copies of TD, to which I have had unmonitored access for more than two weeks.

3. On December 6, 2019 I traveled to the Orange County RCFL for the purposes of initiating several searches in preparation for trial, and to examine the thumb drive sent by the government containing copies of the Virtual Machines (VM) preserving Mr. Erdely's TD validation, performed in my and Atty. Herz's presence, in Anchorage on November 4, 2019. Shortly after arriving at the OCRCFL, my liaison, Joseph Monroe provided to me the aforementioned thumb drive for use on the government-supplied Mac that I have been using to conduct my Anchorage and Orange County examinations. Upon receiving the thumb drive I informed Mr. Monroe that I would like to copy its contents to the aforementioned government computer, so that I can return the thumb drive to his custody, as not to leave it exposed in a shared civilian exam room. As well, VM's typically do not run well, if at all, on external media. Mr. Monroe agreed, so long as it stayed on that computer, as stipulated.

4. Some time later that afternoon, Mr. Monroe re-entered the defense examination room, and informed me that he had received communication from AUSA Jonas Walker, asking him to remind me that I was not to remove anything from that thumb drive from the OCRCFL. I agreed, and reminded him that I had copied its contents to the government's computer, which he acknowledged. AUSA Walker also memorialized this notice in an email on that date at 2:37PM.

5. A short time later, Mr. Monroe again entered the defense examination room and asked if I

had already begun working with the data from the thumb drive. I let him know that I had, but that I also had been having some trouble with errors attributed to an older model computer. Mr. Monroe then informed me that Mr. Walker believed that there may be copies of TD on the thumb drive he supplied, and reminded me that I was not to copy it. I again reminded him that I had already copied the contents of the thumb drive to the government's computer, to remain in RCFL control and custody. He acknowledged that.

6. I left the OCRCFL two different times that day, since having been provided copies of TD. Each time, I left without any search of my property, as is expected when exiting an RCFL facility. (Upon my final exit for the day, Mr. Monroe simply waved from behind glass, and asked if I had anything still running on the computer.) As usual, I had in my possession a laptop, a tablet, a smartphone, and several pieces of removable media which I typically carry in my computer bag. Any one of which could have been used to remove TD from the OCRCFL. Even if I did not already have those storage devices with me, there is a BestBuy directly across the street from the OCRCFL, where I could purchase one. I left the OCRCFL for a lunch break, lasting at least an hour. Plenty of time to purchase removable media.

7. *If* I had nefarious intentions, TD would have *already* been "in the wild" for the past two weeks. I am unsure when Mr. Walker realized that he accidentally sent me two copies of TD, but I presume it was sometime between at least November 19, and December 6, 2019 -- and not likely coincidental with my arrival at the OCRCFL. However, upon realizing that TD was already in my possession, Mr. Walker simply admonished me, via Mr. Monroe, that I was not to remove it from the RCFL, and then trusted me not to. At the October 17-18 and November 26th hearings in Anchorage, it was conveyed to the court that putting TD in my possession is considered to be "in the wild". However, even after realizing that TD had already been released to "the wild", Mr. Walker allowed me unmonitored access to it. At any time, had Mr. Monroe told me that I would not be able to continue my examination due to the accidental release of TD, I would have complied. Instead, I was allowed by the USA to continue my work until standard OCRCFL closing hours, and leave the facility twice -- all the while trusting that I would not remove a copy of TD, or possibly trusting that I was aware of potential consequences

of doing so. Which I am.

8. Simply put, *if* I cannot be trusted with Torrential Downpour, or its secret feature, then both have *already* been irrevocably compromised and released to the wild. And, *nothing* in the government's latest, or even prior proposals will ever get it back. Having earned the respect, not only of defense attorneys, prosecutors, judges, and the media, as well as my entire income for the last quarter century, it is counter intuitive that someone in my position would simply compromise my status for the purposes of aiding criminal behavior. If anything, at least as much as the AUSA and any member of law enforcement, I earn my living *because* individuals are arrested, not because they are empowered to get away with crime. I have every reason, and even several additional legal reasons to keep this software from being compromised. While Mr. Erdely can accidentally reveal a secret TD feature, and Mr. Walker can accidentally release two copies of the software, I would likely be held in contempt of court, at the least, and possibly risk much more. For this reason alone, the government's clear, and demonstrated attempts to thoroughly monitor and collect evidence on me and my examination for the purposes of exposing the breach of a Protective Order, give me pause to consider whether assisting in the defense of one individual may not be worth risking my own career and freedom. I would suspect, given the impositions the government has proposed, very few if any individuals in my position would accept the case.

9. Despite the government's failure to secure its own software and secrets, I have gone to great lengths, both to voluntarily alert the government and the court about information which they accidentally provided to me, as well as to attempt to use equipment owned by the government, at facilities run by the government, and to utilize very expensive specialized hardware and software at my disposal to further reduce the risk of accidental dissemination. To wit, I suggested the use of the LA SCIF, when it was demonstrated to me that the OCRCFL does not physically guarantee the security of equipment and data left in its shared defense exam room.

/ / /

/ / /

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on January 6, 2020.

_____

Jeffrey M. Fischbach

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

ORDER RE MOTIONS FOR RECONSIDERATION

Before the Court at Docket 255 and Docket 256 are the government and the defense's respective Motions for Partial Reconsideration of the Court's order at Docket 254.

BACKGROUND

The factual background of this case is well known to the parties and is condensed here as relevant to the pending motions. On September 12, 2019, the defense filed a motion seeking the production of the Torrential Downpour software.[1] On October 17 and 18, 2019, the Court heard extensive testimony from government and defense experts regarding the materiality of independent defense testing of the Torrential Downpour software. On October 24, 2019, the Court entered an order that granted in part and denied in part the defense's motion

[1] Docket 199.

to compel production of Torrential Downpour.[2] The Court there found that the functionality, reliability, and accuracy of Torrential Downpour were material to Mr. Schwier's defense,[3] but that a validation test performed by the government would be "sufficient to meet the defense's needs" under the balancing test set forth in *Roviaro v. United States*, 353 U.S. 53 (1957).[4]

However, the Court's October 24, 2019, order allowed the defense to file a supplemental declaration of its expert to explain why it believed that additional testing was necessary, and the Court notified the parties that it may amend its order in light of that declaration.[5] On October 31, 2019, the defense filed a supplemental ex parte declaration of Jeffrey M. Fischbach, which described four additional tests he sought to conduct with the Torrential Downpour software.[6] The defense filed a redacted copy of Mr. Fischbach's declaration on the same day, from which it had removed all information claimed as privileged, including the entire

---

[2] Docket 231; *see also* Docket 199 (motion).

[3] Docket 231 at 7–8.

[4] Docket 231 at 10–11. *Roviaro* directs courts determining whether to apply the law enforcement privilege to balance the public interest against the defendant's right to prepare his defense, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors." 353 U.S. at 62.

[5] Docket 231 at 12, 14.

[6] Docket 233.

description of the four tests.[7]

On the government's motion,[8] the Court held a brief status conference on November 4, 2019, after which the parties conducted validation testing of Torrential Downpour pursuant to the October 24, 2019 order.[9] The Court held a second status conference the next day, and on November 8, 2019, ordered the production of Torrential Downpour for defense testing at the Orange County Regional Computer Forensics Lab ("OCRCFL"), "limited to the four tests described in Mr. Fischbach's October 31, 2019 declaration."[10]

The Court's November 8, 2019, order allowed the government to "propose additional terms to the protective order entered at Docket 231 as warranted."[11] The government did so on November 15, 2019,[12] and after yet more briefing, on November 22, 2019, the Court entered a supplemental protective order to govern the defense's testing of the Torrential Downpour software.[13] The order required

[7] Docket 234.

[8] Docket 235.

[9] Docket 243 at 2.

[10] Docket 243 at 2, 7–8.

[11] Docket 243 at 8.

[12] Docket 244. The defense's Response in Opposition is at Docket 248, and the government's Reply is at Docket 253.

[13] Docket 254. The original protective order is at Docket 244.

the government to provide a computer to run Torrential Downpour (the "TD Computer"), while the defense could bring its own computers to connect to the TD Computer with an internet hotspot.[14] Paragraph 6 of the order provided that "[g]overnment personnel will have access to the TD Computer only for the purposes of starting the TD Computer, entering the password for the defense, and keeping the TD [C]omputer secure consistently with OCRFCL standard operating procedures."[15] Paragraph 7 required Mr. Fischbach to install Torrential Downpour onto the TD Computer in the presence of an "FBI agent or Task Force Officer."[16] Paragraph 9 provided that "[t]he TD Computer will contain one network card," and that "[t]he defense will not make any connections to the TD Computer other than through the network card."[17] The November 22, 2019 order did not require the defense to use the packet capture program WireShark during its testing of Torrential Downpour.[18]

The government filed a Motion for Partial Reconsideration at Docket 255,

[14] Docket 254 at 3, 5.

[15] Docket 254 at 4.

[16] Docket 254 at 4.

[17] Docket 254 at 5. Paragraph 8 of the November 22, 2019, Protective Order specified that the defense would be required to connect to the TD Computer using an internet hotspot "that is compatible to connect to the TD Computer via the network card." Docket 254 at 5.

[18] Docket 254 at 2.

requesting that the Court require the defense's use of "Wireshark or another appropriate packet-capture software" to detect whether Torrential Downpour had been copied from the TD Computer.[19]

The defense filed its own Motion for Partial Reconsideration at Docket 256, requesting that the Court amend the November 22, 2019, order to allow Mr. Fischbach to enter the password on the TD Computer himself, install Torrential Downpour without supervision, and to "connect to the TD . . . Computer as necessary to complete its testing."[20]

The Court held a hearing on the parties' cross-motions for partial reconsideration on November 26, 2019. At the hearing, the Court ordered the government to file a response to the defense's motion after it had consulted with the FBI.[21] The Court emphasized at that hearing that it was "not asking the government to propose additional testing," but rather was asking the government "to respond to the defense motion for reconsideration . . . and tell [the Court] what you disagree with and agree with."[22] The Court further explained it sought for the

[19] Docket 255 at 2–4.

[20] Docket 256; Docket 256-1 at 2–3 (proposed order).

[21] Docket 302 at 6:22–9:9.

[22] Docket 302 at 7:15–19.

government "to respond to this issue of WiFi versus Ethernet, the issue of how many access . . . ports into the computer, the issue of the copying as articulated here, and tell me what the government's position is on those."[23] The government responded that the "subject matter experts at the [FBI] . . . [would] need until December 13th to come up with that."[24]

The Court's instructions notwithstanding, the government on December 20, 2019, filed a status report that attached an entirely new proposed testing protocol.[25] As correctly observed by the defense, in filing this proposed new protocol, some three months after the defense motion was filed, and two months after the evidentiary hearing, "[t]he government has seemingly repudiated the testing protocol as provided for in the Court's orders at 231, 243, and 254 the terms of which the government previously had agreed to."[26] The author of the proposed new protocol is not identified; it appears to have been created by one or more

[23] Docket 302 at 8:7–11.

[24] Docket 302 at 8:14–17.

[25] Docket 288. The government's filing incorrectly states "[a]t the hearing on November 26, 2019, the Court ordered the government to submit a revised protective protocol." Docket 288 at 2. By filing a new proposed testing protocol with its response to the defense's Motion for Partial Reconsideration, a full two months after the initial evidentiary hearing regarding defense testing of Torrential Downpour, the government disregarded the Court's clear instruction on the record to restrict its filing to a direct response to the defense's reconsideration motion.

[26] Docket 296 at 2.

unidentified FBI agents.[27] The government states that it is willing to provide testimony from unidentified person(s) to explain its new proposal.[28] The defense filed a response to the government's filing at Docket 296 and an accompanying Supplemental Declaration of Mr. Fischbach at Docket 297. Given this record, the Court declines to consider the government's newest proposed protocol.

Separately, December 19, 2020, the government filed a Fourth Superseding Indictment in the case.[29] The new indictment adds a fourth count to the charges against Mr. Schwier: receipt of child pornography on or about November 18, 2015.[30]

DISCUSSION

The Court will address the parties' respective motions for reconsideration separately, beginning with the defense's motion at Docket 256.

1. Defense's Motion at Docket 256

The defense contends that the November 22, 2019, Protective Order

[27] *See* Docket 288-1 at 1 ("[T]he FBI determined the following test conditions are necessary to sufficiently protect the software from unauthorized disclosure.").

[28] Docket 288 at 2. In a January 13, 2020, Status Report, the government clarified that it would present Detective Erdely "to provide expert testimony regarding the [proposed] Test Environment." Docket 303 at 2.

[29] Docket 279.

[30] Docket 279 at 3.

contains three "manifest error[s] of fact."[31] The defense argues that the first of these is "paragraph 9[,] which limits the defense to the use of one port and network connection" on the TD Computer.[32] The defense maintains that this paragraph prohibitively limits Mr. Fischbach's ability to complete his testing of the software by "prevent[ing] him from installing industry accepted software and hardware as well as well as prevent[ing] him from removing his test results from the [TD Computer] for further examination and analysis on his own equipment."[33] And Mr. Fischbach states in his declaration that he "need[s] access to multiple computer ports and network connections to run [his] tests."[34] The government does not meaningfully respond to the defense's argument. It contends only that the defense's argument is moot in light of the government's new proposed testing protocol, which would allow the defense "to use screens, keyboards, and mice."[35]

Mr. Fischbach, in his declaration, persuasively explains why he requires access to multiple ports on the TD Computer in order to complete the testing

---

[31] Docket 256 at 1–3; *see* L. R. Civ. P. 7.3(h)(1)(A) ("A court will ordinarily deny a motion for reconsideration absent a showing of . . . [a] manifest error of the law or fact.").

[32] Docket 256 at 2.

[33] Docket 256 at 2.

[34] Docket 257 at 8, ¶ 5(e); *see also id.* at 2, ¶ 2.

[35] Docket 288 at 3–4. As noted above, the Court declines to address the new protocol, which it considers to be improperly filed.

authorized by previous order of this Court.[36] And the government has not explained how restricting the defense's access to ports on the TD Computer is necessary to protect Torrential Downpour's integrity as a law enforcement tool. The Court will therefore grant the defense's motion to reconsider with respect to paragraph 9 of the November 22, 2019, protective order.

The defense next argues that "Paragraphs 6 and 7 of the . . . [November 22, 2019,] order . . . compromise attorney-client privilege and attorney work product by intruding upon the confidential and independent defense testing process."[37] The defense contends that Paragraph 6's provision that government personnel start and enter the password on the TD Computer "inserts the government into the defense chain of custody and also makes it impossible for Mr. Fischbach to be held accountable for securing either the [Torrential Downpour] software or his own results as the government now has access to defense work product."[38] The defense maintains that "the only person who should have sole access to defense work product is Mr. Fischbach, and as such he should have sole and exclusive

[36] Docket 257 at 8, ¶ 5(e); *see also id.* at 2, ¶ 2.

[37] Docket 256 at 3. "The work-product doctrine protects 'from discovery documents and tangible things prepared by a party or his representative in anticipation of litigation.'" *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011) (quoting *Admiral Ins. Co. v. U.S. Dist. Ct.*, 881 F.2d 1486, 1494 (9th Cir. 1989)).

[38] Docket 256 at 3.

possession of any passwords."[39] In his declaration, Mr. Fischbach explains that under the terms of Paragraph 6, the personnel responsible for powering on and logging into the TD Computer "would be able to see my examination progress each time they have to log me back into the system . . . , as well as hold exclusive possession of the password to access it while I am away."[40]

The defense further maintains that the way that Mr. Fischbach configures the TD Computer would reveal to a knowledgeable observer information about the type of testing he plans to conduct.[41] The defense therefore contends that Paragraph 7's provision that an FBI agent may observe Mr. Fischbach install Torrential Downpour onto the TD Computer risks divulging privileged information.[42] Mr. Fischbach states in his declaration that "[a] technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct."[43]

The government argues in its response that the defense's assertion of

---

[39] Docket 256 at 3.

[40] Docket 257 at 4, ¶ 5(a).

[41] Docket 256 at 3.

[42] Docket 256 at 3–4.

[43] Docket 257 at 4, ¶ 5(a); *see also id.* at 6, ¶ 5(b) (Mr. Fischbach explaining that configuration of TD Computer would occur before installation of Torrential Downpour and "necessarily make the observing agent privy to attorney client privilege").

privilege is deficient because "Torrential Downpour is the government's software"; because "the presence of the computers and software at the OCRCFL [and] Mr. Fischbach's use of them to prepare for trial . . . are not privileged information"; and because Mr. Fischbach had previously referred to his testing methods as adhering to the "industry standard."[44] The government's argument misses the mark. The defense does not claim that Torrential Downpour itself or the mere use of computers or software at OCRCFL constitute privileged work product. Rather, the defense asserts privilege regarding the tests Mr. Fischbach will perform on Torrential Downpour using that hardware and software.[45] The nature of the tests that Mr. Fischbach intends to conduct on Torrential Downpour and the results thereof are clearly privileged.[46] As the government itself notes, "[t]he work-product doctrine covers documents or the compilations of materials prepared by agents of the attorney in preparation for litigation."[47]

---

[44] Docket 288 at 6–7.

[45] Docket 296 at 8–9.

[46] The Court does not understand Mr. Fischbach to have asserted that the tests themselves were standard, but rather that they complied with industry-accepted standards. *See* Docket 296 at 9.

[47] Docket 288 at 4 (quoting *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011)); *see also Hernandez v. Tanninen*, 604 F.3d 1095, 1100 (9th Cir. 2010) ("The work product doctrine is a qualified privilege that protects certain materials prepared by an attorney acting for his client in anticipation of litigation.").

Mr. Fischbach has persuasively explained that granting the government exclusive password access to the TD Computer and allowing government agents to observe his configuration of that computer would compromise privileged attorney work-product. The government has not introduced evidence to the contrary and maintains only that password-protection is necessary to prevent "the defense from bypassing certain," unspecified, "protections by powering down the computer and then restarting testing without the protections being activated."[48] The Court finds this vague and unsupported assertion unconvincing and will grant the defense's motion with respect to Paragraphs 6 and 7 of the November 22, 2019, Protective Order.

Finally, the defense contends that Paragraph 8's requirement that Mr. Fischbach utilize "an internet hotspot . . . that is compatible to connect to the TD Computer via the network card," is erroneous because "[t]here is no valid basis to restricting the defense to a wired Ethernet connection."[49] The defense requests an amendment allowing Mr. Fischbach to connect to the TD Computer using a standard WiFi connection.[50] The government explained at the November 26,

[48] Docket 288 at 2–3.

[49] Docket 256 at 4.

[50] Docket 256 at 4.

2019, hearing that the term requiring an ethernet connection had been proposed "because [the government's] understanding is it would not be possible for [Mr. Fischbach] to use WiFi at the RCFL," and that "[t]he intent was to identify for him what he would need to do to connect."[51] The Court concludes from this that Paragraph 8's Ethernet requirement serves no valid security purpose, and will therefore grant the defense's motion with respect to the use of WiFi to connect to the TD Computer, to the extent that it is possible to establish a WiFi connection under the OCRCFL's normal operating procedures.

2. Government's Motion at Docket 255

The November 22, 2019, Protective Order did not require the defense to use WireShark during its testing of Torrential Downpour. The Court there explained:

> The government proposes that the protective order contain a term providing that "[a]ll communications with the Torrential Downpour computer will be preserved via Wireshark." The defense objects, contending that "[t]he [C]ourt has no more authority under Criminal Rule 16 to impose a duty on the defense to create evidence than it has to impose such a duty on the government." The Court agrees with the defense on this point, and will not order the defense to use WireShark during its testing of Torrential Downpour.[52]

In its Motion for Partial Reconsideration, the government argues that the protective order "overlooked, and did not address, an important reason the government seeks

[51] Docket 302 at 6:13–18.

[52] Docket 254 at 2 (internal citations omitted).

a protective order with Wireshark or another appropriate packet-capture software: *i.e.* detecting digital copying of Torrential Downpour from the TD Computer."[53]

The Court recognizes the government's concern that "the defense could inadvertently copy Torrential Downpour" onto their own equipment but will not grant the government's motion on this basis. However, the Court finds Mr. Fischbach to be responsible and in possession of technical expertise such that he would be unlikely to unwittingly copy Torrential Downpour and remove it from the OCRCFL.[54] And the Court has expressly ordered the defense not to copy Torrential Downpour and expects compliance with that order. The Court sees no reason to revisit its decision regarding WireShark and will therefore deny the government's Motion for Partial Reconsideration.

3. Miscellaneous Issues Raised in the Government's Response

In addition to responding to the defense's motion for partial reconsideration, the government's response at Docket 288 raises several additional issues. For reasons set out above, the Court will not here consider the government's new

[53] Docket 255 at 2.

[54] A supplemental declaration filed by Mr. Fischbach indicates that the government, itself, believes him to be trustworthy. Mr. Fischbach states that the government inadvertently included two copies of Torrential Downpour on a thumb drive it provided to him on December 6, 2019. Docket 297 at 2, ¶ 2. Mr. Fischbach states that the government, upon realizing this, took no action besides reminding him not to copy the software from the thumb drive. Docket 297 at 2–3, ¶¶ 4–5.

testing protocol, which it proposed a full two months after the Court's first evidentiary hearing regarding the proper environment for defense testing of Torrential Downpour; the Court will, however, address the remaining issues here.

a. Specifications of TD Computer

The November 22, 2019, Protective Order clearly outlines the procedure by which the specifications for the TD Computer would be established. The order first requires the government to provide the defense with "all applicable TD software documentation for versions 1.15 and 1.23, *including installation instructions and minimum operating requirements*."[55] The order next requires the defense to "provide the specifications for the computer that it is seeking for TD testing."[56] Finally, the order requires the government to "provide a government-owned computer . . . that is configured to specifications that were timely provided by the defense."[57] Only "[i]f the defense fails to timely provide such specifications," may "the government . . . select the computer it will provide."[58]

On November 25, 2019, the government provided the defense with a

[55] Docket 254 at 2.

[56] Docket 254 at 2–3.

[57] Docket 254 at 3.

[58] Docket 254 at 3.

redacted user manual for Torrential Downpour version 1.23.[59] Despite the defense's arguments to the contrary,[60] the Court finds that this user manual fulfilled the government's obligation to provide the defense with Torrential Downpour's minimum operating requirements.[61] On December 6, 2019, the Defense timely complied with its obligation to provide the government with system specifications for the TD Computer.[62] Under the terms of the November 22, 2019, Protective Order, the government is now required to provide the defense with a computer that is configured to the specifications supplied by the defense.[63]

The government nevertheless objects to the defense's technical specifications, maintaining that at the November 26, 2019, hearing, "the Court ordered the government to respond to the defense's objections to the computer

[59] *See* Docket 259 (Government's Notice Regarding Partial Compliance with Order (Dkt 254 and Correction of Record). The parties dispute the appropriateness of the government's redactions, *see* Docket 282 (Defense's C-5 Motion to Compel), an issue which the Court will address in a separate order after reviewing the relevant materials in camera.

[60] *See* Docket 296 at 12 n.9 ("The government's claim that it provided software specifications seems disingenuous at best.").

[61] Docket 299-1 at 8 (identifying operating system and programming model required to run Torrential Downpour).

[62] Docket 281-2 at 4. At the November 26, 2019, hearing, the Court extended the deadline to provide these specifications from November 27, 2019, to December 6, 2019. Docket 302 at 10:1–13.

[63] Docket 254 at 3.

the government will provide for testing."[64] The Court disagrees, but has reviewed the transcript for that hearing and understands how the government reached that conclusion.[65] It will therefore address the government's arguments. The government contends that the defense's specifications "are not necessary to operate Torrential Downpour or uTorrent software and to conduct the types of industry-standard tests that the government expects the defense will perform."[66] The government therefore asserts that the defense's specifications "are unreasonable."[67] The government provides no evidence, in the form of a declaration or otherwise, to support its contentions.

As the defense notes, the purpose of the TD Computer is to *test* Torrential Downpour, not to operate it.[68] It is therefore understandable that Mr. Fischbach would require more computing power than is necessary to simply operate the

---

[64] Docket 288 at 9.

[65] Docket 302 at 2:5–5:20.

[66] Docket 288 at 11.

[67] Docket 288 at 10. The government further maintains that "[b]ecause the defense has withheld from the government the specific characteristics of its proposed testing, the government cannot know with certainty what the defense's actual requirements are." Docket 288 at 10. This argument misunderstands the November 22, 2019 order; that order requires the government to provide a computer consistent with the specifications supplied by the defense, not consistent with what the government determines "the defense's actual requirements are." Docket 254 at 2–3.

[68] Docket 296 at 12–13.

software. Mr. Fischbach explains in his declaration that he "specifically chose[]" the specifications to "accommodate the forensic hardware and software [he] need[s] to install in order to both complete [his] testing and assure the [C]ourt that the machine has in no way been compromised during [his] testing, and that no software has been lost, stolen, or compromised."[69] On this record, the Court finds that the specifications provided by the defense on December 6, 2019, are not only necessary for Mr. Fischbach to conduct his testing of Torrential Downpour, but also promote the government's interest in ensuring that the testing is secure.

The Court will therefore order the government to provide the defense with a computer that is configured to the specifications identified at Docket 280-1 page 1, pursuant to the November 22, 2019, Protective Order.

b. Location of Testing

At the November 26, 2019, hearing, the Court directed the government to address whether the defense's testing of Torrential Downpour could occur at the Sensitive Compartmented Information Facility ("SCIF") at the federal building and courthouse in Los Angeles instead of the OCRCFL.[70] Having reviewed the

[69] Docket 261 at 7, ¶ 8.

[70] Docket 302 at 9:13–18.

parties' briefing on this issue,[71] the Court finds that it would not be appropriate to relocate testing to the SCIF. The defense notes that "the government has not raised any objection to moving the testing location to the FBI-Wilshire office," which it asserts "would be a more secure location than the RCFL."[72] If the parties can agree to relocate testing to the FBI-Wilshire office, they can notify the Court and the Court will so order. Unless and until such an agreement is reached, testing will be at the OCRCFL.

CONCLUSION

In light of the foregoing, the government's Motion for Partial Reconsideration at Docket 255 is DENIED. The defense's Motion for Partial Reconsideration at Docket 256 is GRANTED.

The Court will separately issue an amended protective order consistent with this decision.

DATED this 13th day of January, 2020, at Anchorage, Alaska.

s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

[71] *See* Docket 288 at 7–9; Docket 296 at 9–10.

[72] Docket 296 at 10.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

AMENDED PROTECTIVE ORDER

For the reason's set forth in the Court's Order re Motions for Reconsideration,[1]:

1. Not later than January 27, 2020, the government will provide a government-owned computer (the "TD Computer") at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The TD Computer shall be configured to the specifications provided by the defense on December 6, 2019.[2]
2. The only non-government persons who will have access to the TD Computer are Jeffrey Fischbach and Robert Herz

[1] *See* Docket 304.

[2] *See* Docket 280-1 at 1.

(collectively "the defense").

3. Beginning on January 28, 2020, the defense will have access to the TD Computer for 30 consecutive calendar days of testing Torrential Downpour versions 1.15 and 1.23, the versions used in the investigation in this matter. Actual testing days are expected to be Monday through Friday only, exclusive of federal holidays.

4. Government personnel will have access to the TD Computer only for the purposes of keeping the TD computer secure consistently with OCRFCL standard operating procedures. Government personnel will not observe the defense testing.

5. Installation of Torrential Downpour software onto the TD Computer will occur as follows:

   a. An FBI agent or Task Force Officer will keep exclusive possession of a USB drive or other removable media containing the Torrential Downpour software, except as provided in (b) and (c) below. The defense will not possess the Torrential Downpour software, other than on the TD Computer, except as provided in (b) and (c) below.

b. Prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer. The FBI agent or Task Force Officer will remain outside the Defense Review room while Mr. Fischbach installs the software.

c. After the installation, Mr. Fischbach will remove the USB drive or other removable media containing the TD Software from the TD Computer and return it to the FBI agent or Task Force Officer.

6. The defense may bring digital media, computers, cell phones, and an internet hotspot (*i.e*. one that is compatible to connect to the TD Computer via WiFi or a network card) into the OCRCFL room with the TD Computer.

7. The defense will only connect to the TD Computer as necessary to complete its testing. The TD Computer may access the internet through the network card or via WiFi.

8. The defense will not remove the TD Computer from the OCRCFL.

9. The defense will not copy Torrential Downpour to any device

other than the TD Computer. The defense will not receive Torrential Downpour source code.

10. Neither the defense nor the TD Computer will have access to law enforcement's database of hash values from known child pornography images, known as "ICAC COPS."

11. The defense will not tamper with or open the TD Computer.

12. The Court reaffirms its prior protective order, entered at Docket 231.

DATED this 13th day of January, 2020, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

BRYAN SCHRODER
United States Attorney

JONAS M. WALKER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: jonas.walker@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

MOTION TO DISMISS COUNTS 1 AND 2 AND REGULATE PRODUCED DISCOVERY

The United States, through undersigned Assistant United States Attorney, pursuant to Federal Rules of Criminal Procedure 48 and 16(d), moves the Court for an order dismissing Counts 1 and 2 of the Fourth Superseding Indictment and ordering the defense team to certify that they have destroyed all evidence received relating to Torrential Downpour.

A) Reasons for dismissal of Counts 1 and 2

BitTorrent is a peer-to-peer network used by computer-savvy individuals to attempt to hide their receipt and collection of child pornography. Law enforcement officers use Torrential Downpour software to identify distributors of child pornography using the BitTorrent network.

In this case, the Court found "persuasive" the government's evidence that release of Torrential Downpour to the public would undermine the software's effectiveness as a law enforcement tool. *See* Dkt. 231 at 9-10. Over an approximate four-month period, the government has diligently worked to craft testing environments and protective orders with the goals of, both, protecting Torrential Downpour from disclosure, and, also, permitting the defense to prepare for trial, thereby satisfying both United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012), and Roviaro v. United States, 353 U.S. 53 (1957). The United States proposed three protective orders, or terms for protective orders, (Dockets 244-1, 253-4, and 288-1) in its attempt to achieve those objectives.

At Dkt. 304, the Court denied the government's third proposed protective order[1],

[1] At the Final Pretrial Conference on January 14, 2020, the Court indicated that it was persuaded by the defense expert's affidavit (Dkt. 297 at 1-2), which alleged that the government had already released the software by "repeated missteps."

In an abundance of caution, and to ensure clarity in the record, the government respectfully notes that, to the contrary, the government did not err in producing the virtual machines containing the software; rather, it did so pursuant to the Court's order at Dkt. 231.

The affidavit at Dkt. 297 is, apparently, referring to virtual machines produced pursuant to the Order at Dkt. 231, which ordered the validation testing in Anchorage and established the original protective order in this case. Specifically, at Dkt. 231 at 12-13, the Court ordered that "the validation process described at Docket 219-1 shall be carried out

which, in the opinion of the government's subject-matter experts, proposed terms that were essential to protect Torrential Downpour.

The Court gave the government the alternative to "opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense." Dkt. 243 at 7. Under FRCrP 48, "[t]he government may, with leave of court, dismiss an indictment, information, or complaint."

Therefore, pursuant to FRCrP 48, the government respectfully moves the Court to dismiss Count 1 and Count 2 of the Fourth Superseding Indictment.

B) <u>Destruction of sensitive evidence and vacation of pending discovery orders</u>

As indicated in Dkt. 310, the government respectfully requests the Court order that the United States does not have to produce a revised redacted version of the Torrential Downpour manual (per Dkt. 306), nor must it produce the software itself (per Dkt. 305). The government respectfully requests the Court order that the defense file certification that Mr. Herz and Mr. Fischbach have destroyed, and will not access in the future, the Torrential Downpour manuals (including sealed Dkt. 299 and Dkt. 300, and the version produced in discovery); and, further, will not access the virtual machines the government produced to

---

for versions 1.15 and 1.23 of the Torrential Downpour software on November 4, 2019, and on November 5, 2019 as necessary."

Dkt. 219-1 at paragraph 3 includes the following: "Moreover, the computers running the target VM and investigative VM will be available for forensic examination by the defense expert."

Accordingly, the government lawfully produced, per the Order at Dkt. 231, the virtual machines used during the validation testing that was described at Dkt. 219-1. Those virtual machines contained the software.

the defense at the Orange County Regional Computer Forensic Laboratory (OCRCFL), pursuant to the Order at Dkt. 231, and referred to by the defense at Dkt. 297.

RESPECTFULLY SUBMITTED January 23, 2020, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ *Jonas M. Walker*
JONAS M. WALKER
Assistant U.S. Attorney
United States of America

CERTIFICATE OF SERVICE

I hereby certify that on January 23, 2020,
a true and correct copy of the foregoing
was served electronically on the following:

Robert M. Herz
Attorney for Defendant

s/ *Jonas M. Walker*
Assistant U.S. Attorney
Office of the U.S. Attorney

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	)	Case No. 3:17-cr-00095-SLG-DMS

JUDGMENT OF PARTIAL DISCHARGE
RE: COUNTS 1ssss and 2ssss
FED.R.CRIM.P. 32(k)(1)

IT APPEARING that the defendant is now entitled to be discharged for the reason that:

X The court has granted the motion of the plaintiff for dismissal without prejudice of the offenses of Possession of Child Pornography and Distribution and Receipt of Child Pornography as charged in counts 1 and 2 of the Fourth Superseding Indictment.

IT IS THEREFORE ADJUDGED that the defendant is hereby discharged pursuant to Rule 32(k)(1), Federal Rules of Criminal Procedure.

DATED at Anchorage, Alaska, this 3rd day of February, 2020.

S/ Sharon L. Gleason
Sharon L. Gleason
United States District Judge

{DISCHARG-PARTIAL.WPD}

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW SCHWIER, Defendant.	Case No. 3:17-cr-95-SLG-DMS

ORDER GRANTING MOTION TO DISMISS COUNTS 1 AND 2 AND REGULATE PRODUCED DISCOVERY

The Court, having considered the government's Motion to Dismiss Counts 1 and 2 and Regulate Produced Discovery, the defendant's response at Docket 312, and pursuant to Federal Rules of Criminal Procedure 48 and 16(d), ORDERS that:

1. Count 1 and Count 2 of the Fourth Superseding Indictment at Docket 279 are dismissed without prejudice[1];
2. By **February 7, 2020**, the defense shall file a certification that Mr. Herz and Mr. Fischbach:

   a. have deleted, and will not access in the future, the Torrential

[1] *See United States v. Hayden*, 860 F.2d 1483, 1487 (9th Cir. 1988) ("If the district court finds that the prosecutor is acting in good faith in making its Rule 48(a) motion [to dismiss without prejudice], it should grant the motion; conversely, Rule 48(a) empowers the district court to exercise its discretion in denying the motion when it specifically determines that the government is acting in bad faith."). The Court finds the government is acting in good faith in seeking the dismissal of the two TD counts. "[W]hen the government requests a Rule 48(a) dismissal in good faith, the district court is duty bound to honor the request." *Id.* at 1488.

Downpour manual produced in discovery, and sealed Dockets 299 and 300; and

b. will not access in the future the virtual machines the government produced to the defense at the Orange County Regional Computer Forensic Laboratory (OCRCFL), pursuant to the Order at Docket 231, and referred to by the defense at docket 297.

DATED this 31st day of January, 2020 at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE