WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Anthony Espinoza Gonzales, Defendant.	No. CR-17-01311-001-PHX-DGC **ORDER**

Defendant Anthony Espinoza Gonzales is charged with distributing and possessing child pornography in violation of 18 U.S.C. § 2252(a). Doc. 1. The indictment alleges that Defendant distributed child pornography files on eight occasions in December 2016 and January 2017 (counts one through eight), and possessed child pornography on February 8, 2017 (count nine). *Id.* at 1-7.

The Court granted in part and denied in part Defendant's motions to compel discovery relating to the Torrential Downpour software the FBI used in the investigation that led to his indictment. *See* Docs. 25, 51, 54, 86. Defendant has moved for additional discovery relating to Torrential Downpour. Doc. 99. The motion is fully briefed, and the Court held an evidentiary hearing on August 28, 2020. *See* Docs. 102, 107, 111. Computer forensics expert Michelle Bush testified on behalf of Defendant and Detective Robert Erdely testified for the government. For reasons stated below, the motion will be granted in part and denied in part.

I. Background.

A. The BitTorrent Network.

The government claims that Defendant downloaded and publicly shared the charged child pornography files using BitTorrent, an online peer-to-peer network that allows users to download and share files containing large amounts of data, such as movies, videos, and music. To download 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. Once the torrent is downloaded to the BitTorrent client software – in Defendant's case, that software was uTorrent – the software reads the instructions in the torrent, finds the pieces of the target files on the internet from other BitTorrent users who have the same torrent, downloads the pieces, and assembles them into complete files. To share files, the client software makes the pieces of the files accessible over the internet to other BitTorrent users by placing them in a shared folder on the user's computer.

B. Torrential Downpour and the Child Online Protection System.

Torrential Downpour is law enforcement software that uses the BitTorrent protocol. It is part of a suite of law enforcement software that includes Torrential Downpour Receptor and Torrential Downpour, both of which interact with the Internet Crimes Against Children Task Force's Child Online Protection System ("COPS").

Torrential Downpour Receptor roams the internet and queries publicly available BitTorrent indices searching for IP addresses that have made public requests for specified torrents. Some of these torrents are known to include child pornography, and others involve child exploitative activities. Once Torrential Downpour Receptor detects an IP address that has associated itself with a torrent of interest, it reports information about the IP address and the computer's networking port to COPS. This information serves as a lead for officers to investigate using the Torrential Downpour program.

Torrential Downpour is used to contact the IP address and request a download of specific files related to a torrent of interest. The program can interact with COPS in an automated fashion to obtain an investigative lead based on parameters an officer has set in the program, such as a geographic area or a specific torrent. The investigative lead consists of an IP address, networking port, and torrent, all obtained by Torrential Downpour in the manner described above. The IP address and related information are then loaded into the Torrential Downpour program and a contact is initiated. This is how the FBI used Torrential Downpour to contact Defendant's computer. Alternatively, officers can manually input an IP address, networking port, and torrent into the Torrential Downpour program and initiate a contact.

COPS is a database of information from various investigations conducted on several file sharing networks, including BitTorrent. COPS is comprised of several servers and contains "records in" data received from Torrential Downpour Receptor and "records out" data that can be loaded into the Torrential Downpour program through a web portal used by investigating officers. The data in COPS includes IP addresses and the numeric "hash value" – a unique identifier – of torrents being investigated by law enforcement officers around the world. COPS also contains data relating to the identities and IP addresses of investigating officers. COPS is updated by the minute with new information received from Torrential Downpour Receptor.

C. The Government's Use of Torrential Downpour in this Case.

The government alleges that in December 2016 and January 2017, FBI Agent Jimmie Daniels set parameters in his Torrential Downpour program (version 1.33) to automatically request leads from COPS. Doc. 64 at 3-4.[1] Based on these settings, the program automatically downloaded information Torrential Downpour Receptor had collected on Defendant's IP address, networking port, and torrents of interest with which his IP address was associated. *Id.* at 4. Torrential Downpour then connected with

[1] Citations are to page numbers placed at the top of each page by the Court's electronic filing system, not to original page numbers on the documents, if different.

Defendant's IP address, requested files in the torrents of interest, and, the government alleges, downloaded child pornography that Defendant's computer was offering from its shared folder. The government's download of the child pornography is the "distribution" charged in counts one through eight of the indictment. *See* Docs. 1 at 1-5, 64 at 4.

Although Torrential Downpour Receptor was used to identify Defendant's IP address and networking port as points of interest, and reported this information to COPS for further investigation, the government asserts that Agent Daniels did not use Torrential Downpour Receptor in his investigation. Nor were its search results used as probable cause for the search warrant of Defendant's residence. Instead, the actual downloads of child pornography from Defendant's IP address in late 2016 and early 2017, by the Torrential Downpour program, formed the basis for the search warrant. The government states that the search of the internet by Torrential Downpour Receptor will not be used as evidence at trial. *See* Doc. 64 at 4, 7-9, 11, 18.

The search warranted was executed at Defendants' residence on February 8, 2017. Officers found a Microsoft tablet and other computer equipment. Defendant, who lived there with his parents and siblings, stated during an interview that he had used a tablet to find and view child pornography. The tablet was seized and later forensically examined, but the eight files that allegedly were downloaded by Agent Daniels, and that form that basis for counts one through eight of the indictment, were *not* found on the tablet. The name of the torrent for each file was found in the uTorrent AppData folder on his tablet, showing that something had been done with the torrents, but the files themselves were not on the tablet. The government alleges that this evidence is consistent with Defendant having downloaded the files, viewed them, shared them with others (including Agent Daniels) through his shared folder, and then deleted them. The evidence of Defendant having shared them with Agent Daniels is the fact that the government has the child pornography files as they were downloaded from his tablet by Torrential Downpour. The tablet contains other bits of evidence related to the files, including the mention of them in

the jump drive. It also included other child pornography that forms the basis for the possession charge in count nine.

The defense argues that evidence on the tablet is consistent with Defendant having obtained the torrents but never having downloaded the files, or with downloading the files and then immediately deleting them without sharing them with anyone else. In either case, the files would not be found on his tablet and, more importantly, Defendant never would have shared them as charged in the indictment. Defendant notes that the sole basis for the government's claim that he shared the files with anyone is the Torrential Downpour program that allegedly downloaded them from his computer. For this reason, Defendant has sought to test to the Torrential Downpour program to demonstrate that it could have obtained the files from another location and wrongly attributed them to his tablet.

II. The Court's Order on Defendant's First Motion to Compel (Docs. 25, 51).

Defendant moved to compel discovery relating to Torrential Downpour pursuant to Federal Rule of Criminal Procedure 16 and *Brady v. Maryland*, 373 U.S. 83 (1963). Doc. 25. The Court held an evidentiary hearing on January 31, 2019. *See* Doc. 41. Defense expert Tammy Loehrs testified at the hearing in support of the motion. *See* Doc. 50. Agent Daniels testified for the government. *Id.*

In an order dated February 19, 2019, the Court found that Torrential Downpour is material to the defense under Rule 16(a)(1)(E)(i) because the distribution charges are based on child pornography files that Torrential Downpour purportedly downloaded over the internet from Defendant's computer. Doc. 51 at 8-10. The Court denied Defendant's request for an executable copy of Torrential Downpour under *Roviaro v. United States*, 353 U.S. 53 (1957), because the government's investigative efforts would be severely hampered if a copy got into the wrong hands. *Id.* at 14-15. But given the substantial defense interest established by Defendant, the Court concluded that Loehrs should be granted access to Torrential Downpour to assist Defendant in preparing his defense. *Id.* at 15. The Court adopted the Rule 16 disclosure method authorized in *United States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at *8 (D.N.M. Apr. 3, 2013):

> [T]he defense expert [will be permitted] to examine the software at issue at a designated law enforcement facility, at a mutually convenient date and time, for as much time as is reasonably necessary for the expert to complete her examination. No copies of the software shall be made. The software shall not leave the custody of the law enforcement agency that controls it. Any proprietary information regarding the software that is disclosed to the defense expert shall not be reproduced, repeated or disseminated in any manner. Violation of [this] order shall subject the defense expert and/or defense counsel to potential sanctions by this Court.

Id.

Although the Court concluded that Loehrs should be permitted to examine Torrential Downpour given that the charged files were not found on Defendant's computer when it was seized, the Court rejected Defendant's argument that the software is material to a Fourth Amendment challenge because Defendant provided no facts suggesting that the Torrential Downpour searched non-shared space on his computer. *Id.* at 10.

III. The Court's Order on Defendant's Second Motion to Compel (Docs. 54, 86).

On April 15, 2019, Defendant moved to compel the government to comply with the Court's previous order. Doc. 54. The parties had resolved some issues regarding their proposed testing protocols for Torrential Downpour, but disagreed as to whether Loehrs should be permitted to access COPS during testing. *See* Docs. 54-2, 54-3, 54-5. Loehrs proposed to perform nine specific tests: (1) non-parsed torrents, (2) partially-parsed torrents, (3) deleted torrent data, (4) unshared torrent data, (5) non-investigative torrents, (6) files of interest, (7) single-source download, (8) detailed logging, and (9) restricted sharing. Doc. 56-1 at 21-24. "Non-parsed," as used in Loehrs's proposal, means torrents that have been downloaded but not executed or fully executed – meaning the user has not yet triggered the torrents to go on the internet and download the actual video files. As proposed by Loehrs, tests one through six would each conclude with a search of COPS for any investigative hits on the suspect IP address and determine whether the Torrential Downpour program attempts to connect with that address to download data. *Id.* at 21-23.

The Court held an evidentiary hearing on August 16, 2019. *See* Doc. 82. Loehrs testified on behalf of Defendant. *See* Docs. 82, 87. Detective Erdely, who helped create

Torrential Downpour and is the current administrator of COPS, testified for the government. *Id.*

In an order dated August 27, 2019, the Court denied Defendant's motion with respect to tests one, two, five, and six, and granted the motion with respect to tests three and four. The government had already agreed to tests seven, eight, and nine. Doc. 86. Tests one and two were deemed unnecessary because the government conceded that Torrential Downpour Receptor will identify non-parsed and partially-parsed torrents of interest – the very facts the tests were designed to establish. *Id.* at 7-10. This concession is material to the defense because it shows that an IP address can be identified by Torrential Downpour Receptor as an investigative lead if it has a torrent of interest but does not have the actual files associated with the torrent. Thus, Defendant's tablet could have been identified as an investigative lead by Torrential Downpour Receptor if it had the torrents of interest but not the related child pornography, as was true when the tablet was seized by investigators. Stated differently, given the government's concession on tests one and two, the fact that Defendant's tablet was identified as an investigative lead by Torrential Downpour Receptor does not show that it ever contained the child pornography alleged in counts one through eight of the indictment.

The Court permitted Defendant to conduct tests three and four, without access to COPS, to determine whether the Torrential Downpour program can access deleted or unshared torrent data. *Id.* at 10-11. The act of distribution charged in this case is Defendant's allegedly having placed child pornography in the shared folder of his uTorrent software for others to download. *See United States v. Budziak*, 697 F.3d 1105, 1109 (9th Cir. 2012) (holding that evidence is sufficient to support a conviction for distribution "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."). If Torrential Downpour obtained the child pornography from non-shared space on Defendant's tablet, then he did not engage in the act of distribution (placing the files in shared space) with which he is charged.

The Court denied Defendant access to COPS for tests three and four because Defendant failed to show that such access was necessary to perform the tests or material to preparing the defense as required by Rule 16. *Id.* at 15-16. The Court also concluded that COPS is protected from disclosure by the *Roviaro* privilege and that the government should not be forced to incur the substantial time and expense required to recreate the COPS database for Defendant's investigation, as Loehrs had proposed. *Id.* at 16-17.

The Court denied tests five and six because whether Defendant's IP address was identified by Torrential Downpour Receptor based on lawful files is not material to the defense. Also, the government acknowledged that Torrential Downpour Receptor may look at associations with lawful torrents that have some connection to child pornography, and that Torrential Downpour will sometimes download lawful files while investigating torrents of interest. *Id.* at 12-13.

Tests seven, eight, and nine were not at issue in the hearing because the government agreed Defendant could perform them, and none of them required access to COPS.

IV. The Test Results and Defendant's Requested Additional Testing.

Although his motion is not entirely clear, Defendant made clear at the August 28, 2020 hearing that he now seeks three additional tests: (1) further single-source testing, (2) tests run with Torrential Downpour and the COPS data base, and (3) comprehensive independent testing of Torrential Downpour by an outside firm other than Loehrs. The Court will address his request for additional single-source testing in this section, and his other two requests in the following sections.

Defendant's testing of Torrential Downpour occurred at an FBI office in Phoenix on October 7-9, 2019. Loehrs and her colleague Michele Bush operated a computer (the "suspect computer") using uTorrent software, the same BitTorrent client software that was on Defendant's tablet. FBI Agent Brian Wade operated a government computer with Torrential Downpour version 1.33 installed ("the government computer"), the version used by Agent Daniels in this case. Wireshark packet capture software was used to record the

transfer of data. Agent Wade prepared a 14-page report documenting his observations of the testing. Doc. 99-2. Loehrs produced a 148-page report. Doc. 99-1.

B. Tests Three and Four – Deleted Files and Files in Non-Shared Space.

Tests three and four involve scenarios where the suspect computer executes a torrent and downloads its files from the internet, and the files are then either deleted from the suspect computer or moved to non-shared space on the computer. Docs. 56-1 at 21-22, 99-1 at 6. The government computer, through Torrential Downpour, then attempts to make a connection with the suspect computer and download the files. The relevant question, for reasons explained above, is whether Torrential Downpour can download deleted files or files in non-shared space.

To start test three, a control test was conducted. Bush used the uTorrent software on the suspect computer to download a non-contraband file from the internet. Agent Wade then used Torrential Downpour on the government computer to connect to the suspect computer over the internet and successfully downloaded the non-contraband file. Doc. 99-2 at 3-4. This proved that the government computer could connect to the suspect computer using Torrential Downpour and download a BitTorrent file.

Bush and Loehrs then ran eight tests in which they used the suspect computer to download a non-contraband file from the internet and then deleted the file from the suspect computer in various ways – deleting it but leaving it in the recycle bin, deleting it completely, deleting it from within the uTorrent program, deleting it outside of the uTorrent program, etc. In each test, Wade used Torrential Downpour to attempt to download the file from the suspect computer after it had been deleted. In each instance, Torrential Downpour was unable to download the file. *Id.* at 4-6. This demonstrated that Torrential Downpour does not download a file from a suspect computer once the file has been deleted.

Test four was designed to determine whether Torrential Downpour can download a file from non-shared space on a suspect computer. Eight tests were conducted. In each, Bush downloaded a non-contraband file from the internet and then moved the file from shared space to non-shared space on the suspect computer. This involved moving the file

from the shared folder to the program file directory, to a virtual hard disk, to an encrypted storage container with a password, to the root directory, etc. After the file had been moved, Agent Wade used Torrential Downpour to attempt to download the file from the suspect computer. In each of the eight instances, Torrential Downpour could not download the file. *Id.* at 7-10. This demonstrated that Torrential Downpour does not download a file that has been moved from the shared folder on the suspect computer.

Even though Torrential Downpour was unable to download the file in any of the scenarios in tests three and four, Loehrs concluded in her report that test three had a 10% percent failure rate and test four had a 40% failure rate. Doc. 99-1 at 6. The "failure" in test three occurred in the seventh scenario and was explained this way by Loehrs: "the Suspect Computer deleted the payload of a torrent and Torrential Downpour still successfully connected to the Suspect Computer and identified the suspect as being in possession of the torrent after it was deleted." *Id.* The failure in test four was explained the same way: "the data of the payload was unshared using various methods but Torrential Downpour still successfully connected to the Suspect Computer and identified the suspect as being in possession of the torrent after it was unshared." *Id.*

As the government notes, however, it is important to distinguish between the first connection between Torrential Downpour and the suspect computer, where a connection is made and Torrential Downpour learns whether the suspect computer has some or all of the file it is seeking, and the actual download of the file. In the tests where Loehrs claims a failure, the connection was made and Torrential Downpour reported that the suspect computer had the files, but then was not able to downloaded the files, a fact agreed to by defense counsel at the recent hearing. Torrential Downpour did not obtain the files from the deleted or non-shared space in any of these tests.

Detective Erdely explained in a detailed declaration and during his hearing testimony that the initial connection, in which Torrential Downpour connects with the suspect computer and learns whether it has the files being sought, does not involve Torrential Downpour looking into the suspect computer's non-shared spaces. Rather, the

uTorrent software in the suspect computer reports on the files it possesses. If the files have been deleted or moved to non-shared space from outside of the uTorrent software, then the software will not know they have been moved or deleted and will report them as present. It will not know they have been deleted or moved until an actual download is attempted. Thus, when Bush, working outside of the uTorrent software, deleted or moved the non-contraband file to non-shared space before Torrential Downpour made its connection with the suspect computer, the uTorrent software in that computer reported the files as available to be shared – the last information it had obtained before the connection was made. This is a portion of Erdely's explanation:

> [Torrential Downpour] accurately reported the information that was received from uTorrent (suspect computer). uTorrent explicitly notified Torrential Downpour that it possessed all of the pieces/files. This behavior is consistent with how uTorrent would behave with other BitTorrent clients. . . . Torrential Downpour simply reported the messages received from uTorrent. Therefore, there was no error – Torrential Downpour properly recorded the "Piece Exchange" which was sent by the suspect computer (uTorrent). This information is used to inform the BitTorrent programs, what pieces were available for sharing. After the piece exchange is completed, BitTorrent programs can request any of the pieces the sharing client has reported as being available. If the data is no longer available to be shared, no data is sent.

Doc. 102-1 at 7.

Erdely further explained why the suspect computer's uTorrent program was not aware that files had been deleted or moved to non-shared space:

> It is important to understand that Loehrs Forensics tested files they deleted, moved or made unavailable some other way from *outside* of the uTorrent Program. It should be noted that uTorrent provides a method to stop sharing by deleting the files from *within* the program, which was known to the uTorrent program immediately by the fact that pieces were exchanged after deleting and no errors were reported. But, the tests where Loehrs Forensics reported an error, the files were moved, deleted or made unavailable *outside* of the running program. In other words, uTorrent would not be aware that the files were no longer available until uTorrent attempted to access those files.

Id. (emphasis in original).

Erdely provided computer readouts from the tests performed by Loehrs and Bush that show, in each alleged "failure," that the "have-all" files message – which indicates that the sought-after files are present and available for download – was sent by the suspect computer's uTorrent software to Torrential Downpour during the initial connection. *See* Doc. 102-1 at 7-20. It was not obtained by Torrential Downpour searching the suspect computer. And when the actual download was attempted, no files were transferred because they had been deleted or moved from the shared folder. In other words, in each of the tests run by Defendant's experts, Torrential Downpour performed as the government claims: it did not download files that had been deleted or moved to non-shared space.

During the hearing, Michelle Bush agreed with Erdely's explanation of what happened. She confirmed that it was the suspect computer that reported the file was present for download, and that the message was duly recorded by Torrential Downpour. She agreed that the file was not actually downloaded by Torrential Downpour because it was not available, having been deleted or moved to non-shared space. But she continued to characterize this as an error in Torrential Downpour. She asserted that Torrential Downpour recorded inaccurate information when it initially noted that the file was available on the suspect computer for sharing.

The Court cannot agree that tests three and four revealed a flaw in Torrential Downpour. It was the suspect computer, not Torrential Downpour, that reported the file was available for download when it was not, a report Torrential Downpour accurately recorded. And more importantly, Torrential Downpour never downloaded a file that Bush had deleted or moved. The tests thus confirm that if Torrential Downpour downloads files from a suspect computer, it does so because the files are in the shared space, available for download – the act of distribution alleged in this case.

Defendant has proposed no specific additional testing related to non-shared space, but his broad requests for testing with COPS and independent testing of Torrential Downpour by an outside firm presumably would include this issue. The Court concludes,

however, that no further non-shared space testing is warranted. Tests three and four were designed by Defendant's experts and confirmed in each instance what the government has represented about Torrential Downpour – that it does not somehow enter non-shared space to download files.

In his initial motion to compel, Defendant argued that Torrential Downpour commits a Fourth Amendment violation because the program "searches beyond the public domain, essentially hacks computers searching for suspect hash values, and therefore conducts a warrantless search[.]" Doc. 25 at 6. The Court rejected this argument because Defendant identified no evidence that Torrential Downpour accessed non-shared space on his computer and, as discussed in more detail in the Court's previous order, Defendant "must make a 'threshold showing of materiality'" to obtain discovery under Rule 16(a)(1)(E). *Budziak*, 697 F.3d at 1111 (quoting *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 Government is in possession of information helpful to the defense.'" *Id.* at 1112 (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)) (emphasis added). Defendant still has identified no such evidence.

Defendant's motion will be denied to the extent he seeks to perform additional testing related to non-shared space or a potential Fourth Amendment challenge.

C. Test Seven – Single-Source Download.

Loehrs proposed test seven to determine whether Torrential Downpour in fact limits its downloads to a single IP address. Doc. 56-1 at 23. The question test seven seeks to answer is not whether Torrential Downpour can conduct a single-source download, but "whether Torrential Downpour will obtain files from other sources when it is unable to conduct a single-source download." Doc. 99-1 at 6-7.

Test seven involved six steps: (1) execute and run BitTorrent software from the suspect computer; (2) initiate the download of at least one non-contraband torrent of interest from the internet; (3) execute and run Torrential Downpour from the government

computer; (4) pause all torrent downloads before the download process completes; (5) allow the suspect computer and government computer to run for at least 10 minutes or until a connection is made; and (6) review all packet captures between the government computer regarding the connection with the suspect computer for the identified torrent to determine if all data originates from the suspect computer. Doc. 99-1 at 78-79. These were the steps originally proposed by Loehrs. *See* Doc. 54-4 at 14.

During the testing in October 2019, test seven was executed 10 times with successful connections between the suspect and government computers being made each time. *Id.* at 79. The testing resulted in no obvious failures, meaning Torrential Downpour did not connect to other IP addresses to download data when the data was unavailable on the suspect computer. *Id.* at 7; *see* Doc. 99-2 at 11-15. Loehrs nonetheless deems test seven "incomplete and inconclusive" because, she asserts, it was given no opportunity to fail. She argues that "Torrential Downpour was manually directed to connect only to a single IP address with no possibility of connecting to other sources or concurrently investigating different suspects." Doc. 99-1 at 7.

Erdely asserts that Torrential Downpour is always given only one IP address to which to connect. Doc. 102-1 at 24. He further asserts that during the Loehrs-designed tests the government computer and suspect computers made their connection over the internet. The government computer thus had the opportunity to search the internet for additional downloads when it could not complete the download from the suspect computer, but it did not do so. And we know the non-contraband file was available at other locations on the internet because it was downloaded by the suspect computer from the internet at the start of each test. The fact that the file was not downloaded confirms, in Erdely's opinion, that Torrential Downpour makes only single-source downloads. *Id.*

In their briefing and during the hearing, the defense did not suggest that test seven revealed any weakness in Torrential Downpour. Instead, the defense suggested that test seven, even though designed by Loehrs, was insufficient to truly determine whether Torrential Downpour always downloads from a single source.

Bush testified that when Torrential Downpour connects to a single IP address, there may be multiple computers at that IP address – such as multiple computers in a home or on an office network – and Defendant should be allowed to test whether Torrential Downpour can blur the distinction between these computers, attributing a download from one computer in a house to another computer in the house.

In response, Erdely testified that this is why Torrential Downpour obtains not only an IP address, but also a networking port number. He explained that each device at a specific IP address connects to the internet through a networking port that is separate from another computer's. If two or more computers are connecting to the internet from a single IP address, a separate networking port exists for each and a separate TCP connection is made for each.[2] One court explained TCP connections in this way:

> TCP is a protocol layered on top of IP to provide reliable bidirectional communications. TCP connections are established through a three-part handshake, after which messages may be transmitted in both directions. The first message in that handshake is sent from the source to the destination, and serves to initiate the TCP connection. The destination replies, and the source confirms the reply. After that, the data may flow in either or both directions until the TCP connection is terminated.

USA Video Tech. Corp. v. Movielink LLC, 354 F. Supp. 2d 507, 516 (D. Del. 2005) (citation and ellipses omitted).

Erdely explained TCP connections are created and controlled outside of Torrential Downpour – such as by Windows operating software – and that that they do not overlap or blur into each other. The example he provided was simultaneous connections from a home computer to CNN and another news service such as ESPN. A separate TCP connection will be made for each news service, even though they both are using the same IP address, and the communications will not blur or merge into each other – the user won't get CNN content on the ESPN connection.

---

[2] "TCP" stand for "Transmission Control Protocol."

Bush agreed with this explanation of how Torrential Downpour communicates with suspect computers. She also agreed that the TCP connection is made and managed by software other than Torrential Downpour.

Bush further asserted that Torrential Downpour has the ability to conduct multiple searches at one time, and that the defense should be permitted to test whether the results of such simultaneous searches can blur together – whether a file downloaded in one search can be attributed by Torrential Downpour to a suspect computer in another simultaneous search.

Erdely testified that Torrential Downpour can conduct multiple simultaneous searches, that each focuses on a single IP address and networking port, and that each occurs through its own TCP connection. He testified that each search can be seen at the top of the Torrential Download computer page as a tab, just like a computer that is simultaneously connected to CNN and ESPN will have separate tabs and separate TCP connections.

In light of Erdely's undisputed testimony that Torrential Downpour establishes a separate TCP connection for each suspect computer at an IP address or for each suspect computer in simultaneous searches, it seems highly unlikely that blurring between the TCP connections could occur. But the government's claim that Torrential Downpour can download only from a single source is at the heart of this case, given that none of the videos charged in counts one through eight were found on Defendant's tablet. The government will rely on the single-source feature of Torrential Downpour to assert at trial that the downloaded videos came from Defendant's device and nowhere else. As a result, the Court concludes that Defendant should be allowed the two additional tests Bush mentioned: (a) a test to determine whether Torrential Downpour can blur between multiple computers at a single IP address, and (b) a test to determine whether it can blur between suspect computers in multiple searches being conduct simultaneously by Torrential Downpour.

The parties shall confer in good faith regarding the protocols for these additional tests. The testing shall be completed no later than **October 2, 2020**. Defendant's motion for additional discovery will be granted in this regard.

D. Test Eight – Detailed Logging.

Loehrs proposed test eight to determine "the accuracy of Torrential Downpour's logging feature[.]" Docs. 56-1 at 23, 99-1 at 86. The test involved six steps: (1) execute and run the publicly available BitTorrent software from the suspect computer; (2) initiate the download of at least one non-contraband torrent of interest; (3) execute and run Torrential Downpour from the government computer; (4) continue downloading non-contraband torrent of interest on the suspect computer; (5) allow the suspect computer and government computer to run for at least 10 minutes or until a connection is made; and (6) compare the "details.txt log" with the information from the suspect computer to determine if the total number of pieces, number of pieces possessed, software version, and pieces downloaded are accurately logged. *Id.*

Test eight was performed using 10 different torrent files. Docs. 99-1 at 86-134, 99-2 at 11. According to Loehrs, the testing resulted in no obvious failures in reporting IP addresses, networking ports, torrent specifications, and hash values. Doc. 99-1 at 7. But Loehrs's report notes that in tests using deleted or non-shared files, the Torrential Downpour log files reported that the suspect computer "'has all the files, based on pieces acknowledged' when the file was indisputably deleted or unshared." *Id.* Loehrs deems test eight "incomplete and inconclusive" because it "cannot account for the log files misrepresenting information on a suspect computer[.]" *Id.*

As discussed above, however, Erdely demonstrated and Bush agreed that the presence of the files was reported by the suspect computer's uTorrent software; it was not determined by Torrential Downpour. The Torrential Downpour logs accurately recorded what the uTorrent software reported, even if the report was inaccurate. When the download was attempted, Torrential Downpour did not receive any files that had been deleted or moved to non-shared space. The results of test eight do not warrant further testing.

E. Test Nine – Restricted Sharing by Torrential Downpour.

Test nine was designed to determine whether the Torrential Downpour program distributes files to the internet. The government claims that the program, unlike other

BitTorrent programs, does not make downloaded files available for other BitTorrent users to download.

Loehrs reported that the test "received a score of 100%," meaning that "no evidence was found that Torrential Downpour distributed data back out on the BitTorrent network." Doc. 991 at 7. The report notes that the test was not run in an automated state and did not determine whether Torrential Downpour distributes files to COPS or other IP addresses, but Defendant has not proposed other specific tests on this issue and the results of test nine do not warrant any.

V. The COPS Database.

Defendant contends that testing with the COPS database is required under Rule 16 because testing performed to date verifies that COPS "is an integral and essential component of the [Torrential Downpour] software and must be included in testing in order to satisfy industry standards regarding function and accuracy." Doc. 99 at 14. Defendant quotes this portion of Loehrs's report in support of his contention:

> [U]pon learning that references to the ICAC COPS database is contained within actual system files of the [Torrential Downpour] software, it is reasonable to assume that it must also be contained within the source code. If this is true, it would be fundamental to the testing process to analyze the source code to determine the importance of the ICAC COPS database as it relates to the overall functionality of the Torrential Downpour software. For example, if Torrential Downpour is unable to obtain a file from the suspect, ICAC COPS could potentially intervene to obtain the file from its own database or send instructions to the Torrential Downpour software to obtain the file from other IP addresses.

Id. (quoting Doc. 99-1 at 9). Defendant speculates that "COPS *could* instruct Torrential Downpour to access other computers to obtain the illegal parts of the torrent[,]" and if "Torrential Downpour locates only the hash value of an illegal file, but not the file itself, . . . COPS *could* obtain those illegal files from its own database." *Id.* at 15 (emphasis added). Defendant claims that these "possibilities" must be considered given that none of the files charged in counts one through eight was found on his tablet. *Id.*

Mere possibilities do "not satisfy the threshold showing of materiality required for production under Rule 16(a)(1)(E)(i)." *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1004 (D. Ariz. 2012) (citing *Mandel*, 914 F.2d at 1219); *see United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995) ("[Defendant's] assertions, although not implausible, do not satisfy the requirement of specific facts, beyond allegations, relating to materiality."); *United States v. Griffin*, No. CR 02-938(A)-RGK, 2006 WL 8429329, at *3 (C.D. Cal. Oct. 20, 2006) ("[Defendant's] allegations are based on speculation, but that is insufficient to establish materiality under Rule 16."); *United States v. W. R. Grace*, 401 F. Supp. 2d 1069, 1085 (D. Mont. 2005) ("[S]peculation falls short of showing 'facts which would tend to show that the Government is in possession of information helpful to the defense,' as is required by Rule 16.") (quoting *Santiago*, 46 F.3d at 894).

What is more, the Court has concluded that COPS is protected from disclosure by the *Roviaro* privilege because the government has a legitimate interest in preserving its ability to investigate and prosecute the distribution of child pornography, and because COPS contains highly sensitive information about thousands of ongoing investigations into child pornography worldwide, including hash values for torrents of interest and the IP addresses of both suspects and investigating officers. Doc. 86 at 16 (citing Doc. 64 at 12). As Erdely stated in his declaration:

> ICAC Cops contains the search results of law enforcement officers who are trained to use it, and acts as a case coordination and case tracking tool. ICAC Cops includes critical details of active investigative data like the Internet Protocol (IP) address(es) and physical addresses of the officers, as well as the IP address(es) and physical addresses of users being investigated for distributing and receiving child exploitative material.

Doc. 102-1 at 2.

Defendant's speculation that COPS "could" obtain files from its own database or instruct Torrential Downpour to obtain files from other IP addresses is not sufficient to overcome the *Roviaro* privilege. *See Rigmaiden*, 844 F. Supp. 2d at 1004. Defendant's motion will be denied with respect to the disclosure of COPS.

VI. Independent Testing of Torrential Downpour and COPS.

Defendant requests an order requiring "industry standard testing" on Torrential Downpour and COPS. Doc. 99 at 2, 16; Doc. 107 at 2. When the Court asked defense counsel at the hearing what authority Rule 16 provides for this Court to order the government to have its programs independently tested, he could identify none. The Court has reviewed Rule 16(a) and can find no such authority. The rule requires the government to produce various categories of information in its possession, but does not require it to undertake actions it has not already undertaken. Defendant can argue at trial that the government has never had Torrential Downpour or COPS independently tested, but it cannot force the government to undertake such testing.

Defense counsel suggested that the testing could be arranged and paid for by the defense. But this would require the government to provide an installable copy of Torrential Downpour and COPS for testing by a third-party. Defendant previously made this request regarding Torrential Downpour, and the Court denied it on the basis of *Roviaro*. *See* Doc. 51 at 13-15. The Court concluded that the Loehrs testing it permitted served Defendant's interests, and that further disclosure was not warranted when Defendant's interest (with the Loehrs testing) was balanced against the government's interest in maintaining the confidentiality of Torrential Downpour. *Id.* The Court reaches this conclusion again. The defense testing conducted to date does not cast doubt on the government's representations regarding Torrential Downpour. If anything, it supports those representations. The Court will allow limited additional testing of Torrential Downpour's single-source download feature as discussed above, but concludes that disclosure of an installable copy of Torrential Downpour or COPS is not warranted for the reasons previously explained. *Id.*

VII. Conclusion.

As the Court expressed at the August 28 hearing, it is concerned about the length of time this case has been pending. Some delay was occasioned by the testing that has occurred, and some by the change of defense counsel earlier this year. But the Court

concludes that the parties have had ample time to prepare this case and that a trial should be scheduled and held as soon as the testing allowed in this order is completed and public health conditions allow.

IT IS ORDERED:

1. Defendant's motion to compel additional discovery (Doc. 99) is **granted in part and denied in part** as set forth in this order. The parties shall promptly confer in good faith and settle on protocols for the additional testing of a single-source download: (a) a test to determine whether Torrential Downpour can blur between multiple computers at a single IP address, and (b) a test to determine whether it can blur between suspect computers in multiple searches being conduct simultaneously by Torrential Downpour. The testing shall be completed no later than **October 2, 2020**.

2. Excludable delay pursuant to 18 U.S.C. § 3161(h)(1)(D) is found to run from May 1, 2020. *See* Doc. 99.

Dated this 1st day of September, 2020.

David G. Campbell
Senior United States District Judge