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