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