IN THE UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

HOCK CHEE KOO, THONGSOUK SOUTAVONG, et al.,

Defendants.

Criminal Case No. 09-321-(2,3)-KI

OPINION AND ORDER

Dwight C. Holton
United States Attorney
District of Oregon
Gregory R. Nyhus
Assistant United States Attorney
1000 SW Third Avenue, Suite 600
Portland, Oregon 97204-2902

Attorneys for Plaintiff

Christopher J. Schatz
Rubin L. Iniguez
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, Oregon 97204

Attorneys for Defendants

KING, Judge:

Pending before the Court are the following two motions filed by defendants Hock Chee Khoo and Thongsouk Soutavong: Motion to Exclude Images of the Wu Laptop and External Hard Drive (#34) and Motion to Compel Government to Extend Use Immunity to Brian Emerson (#40). A third defendant, Shengbao Wu, has not appeared in the case. For the following reasons, I grant in part and deny in part the Motion to Exclude Images and I deny the Motion to Compel Use Immunity.

BACKGROUND

I. Procedural Background

Soutavong and Khoo are each charged with one count of conspiracy in violation of 18 U.S.C. § 371 (alleging Intent to Commit Wire Fraud, 18 U.S.C. § 1343, Theft of Trade Secrets, 18 U.S.C. § 1832, and Fraud in Connection with Computers, 18 U.S.C. § 1030(a)(4)). Khoo and Soutavong are also charged with three substantive counts of wire fraud in violation of 18 U.S.C. § 1343, and Soutavong is charged with three substantive counts of theft of trade secrets in violation of 18 U.S.C. § 1832. Wu is charged with the same conspiracy, as well as six substantive counts of theft of trade secrets and two counts of fraud and related activity in connection with computers in violation of 18 U.S.C. § 1030. Finally, the indictment provides

that the alleged conspiracy included "defendants WU, SOUTAVONG and KHOO, *and others known and unknown* to the grand jury." Indictment at 2 (emphasis added).

At an evidentiary hearing, I heard testimony from FBI Special Agent George Chamberlin, Lawrence Andrew Hoffman, FBI Special Agent Phil Slinkard, Michael Bean, and Portland Police Officer Steven Johns on the Motion to Exclude Images, and I requested that the parties submit their closing arguments in writing. I also heard argument on the Motion to Compel Use Immunity and took that motion under advisement. I ruled on the other pending motions, the results of which are captured in a minute order at docket # 84.

II. Factual Background

The following facts were adduced from testimony and evidence presented at the evidentiary hearing:

Defendants' charges arise out of their alleged attempt to compete with their employer The Hoffman Group, a manufacturer and distributor of after-market auto parts. In September of 2006, Lawrence Hoffman, owner of The Hoffman Group, discovered a product for sale on eBay that looked like a type of automobile part his company sold. The product was a vertical door lift. The eBay part was offered under the brand name "Cleanline Motor Sports," which was registered by a company called "JES Suppliers, LLC." The Hoffman Group's part was called the "130 Degree Lambo Vertical Door Kit."

Hoffman alerted his company's attorney, John Ramig, and began investigating JES Suppliers, LLC. He learned that it had been incorporated in Oregon on May 18, 2006 by Wu, Soutavong, and Khoo. At that time, Soutavong worked for Hoffman's company in sales and Wu

worked for a subsidiary in China, managing the design and manufacture of products there. Khoo was a former employee, who had worked in warehouse and shipping.

On September 12, 2006, Ramig and Hoffman reported what they knew to the FBI's SA Slinkard. Hoffman hired a private investigator who purchased the JES part and learned that it was identical to The Hoffman Group's part. The private investigator also emailed Wu and Khoo acting as a potential business partner. Hoffman later testified (in a civil action brought by his company) that Wu sent images to the private investigator of products and parts that The Hoffman Group had not yet released.

On October 16, 2006, The Hoffman Group filed a civil complaint against Wu, Soutavong, Khoo and Brian Emerson (who was initially identified as "John Doe") in Multnomah County Circuit Court. Until August 5, 2006, Emerson had operated The Hoffman Group's computer system, with administrator privileges on the computer network. Hoffman believed Emerson had given the other defendants access to The Hoffman Group's computer data management application, Platipus. The Hoffman Group alleged in the lawsuit that the defendants had obtained and used confidential information and trade secrets to divert business from The Hoffman Group.

On October 17, 2006, at Hoffman's request, Wu traveled from China to the United States. Hoffman met Wu at the airport, took him back to the office, and asked Wu to leave his laptop computer (company-owned) with Mark Hansen. Hoffman told Wu that Hansen was a company employee who would upgrade Wu's computer.

In fact, Hansen worked for Northwest Countermeasures as a computer analyst whom Hoffman had hired to examine Wu's laptop. When Hoffman and Wu had left the room, Hansen

opened a folder named "private" and moved it to the laptop desktop. Hansen then copied selected parts of the "private" folder onto a USB external hard drive device using Acronis software (hereinafter the "Acronis Backup"). This "private" folder purportedly contained documents relating to JES Suppliers, LLC.

Hoffman took the laptop home and, over the course of two days, periodically booted it up and looked around. He testified he "could have" moved files, but did not delete files and did not run the defragmentation utility. Tr. 71, 64.[1] He made "screen shots" of a chat program contact list, which he saved to a subfolder in the "private" folder he named "QQ."

Hoffman contends that the "private" folder contained trade-secret protected information owned by The Hoffman Group. The "private" folder also contained a Filemaker software database, or a computer data management application, known as "Platipus." Hoffman had apparently customized Platipus for The Hoffman Group's use.

On October 18, 2006, Hoffman terminated Wu and Soutavong's employment.

On October 20, 2006, Hoffman brought Wu's laptop to the FBI. Until then, the FBI had no idea Hoffman had seized Wu's laptop and imparted no advice or guidance to him about how to seize it. Hoffman told SA Slinkard he had booted the laptop up and looked through files while he had the laptop at home. With SA Slinkard watching, Hoffman turned the computer on and copied the "private" folder to an external Western Digital USB disk drive. Hoffman gave the computer and the Acronis Backup to SA Slinkard. Slinkard checked both into the evidence system on October 20, after which he submitted them to the Northwest Regional Computer

---

[1]"Tr." refers to the transcript of the December 6, 2010 evidentiary hearing, available at docket #93.

Forensic Laboratory ("NWRCFL") for examination. Tr. 104. The Acronis Backup and laptop were checked into the NWRCFL's laboratory on November 1, 2006. Between November 3 and November 6, FBI Special Agent Joel Brillhart made an image of the laptop using Forensic Tool Kit software (hereinafter the "Laptop Image") and an image of the Acronis Backup (hereinafter the "Acronis Backup Image"). The FBI kept these *images*, but returned the actual laptop and the Acronis Backup to Hoffman on November 20, 2006.

In February of 2007, the government interviewed Hoffman to evaluate any financial losses to his company caused by Wu, Soutavong, Khoo and Emerson. Ramig contacted AUSA Greg Nyhus to evaluate whether the defendants could be criminally charged.

Emerson investigated the allegations in order to defend himself in the civil action, and began assisting the government at the same time. Emerson met with SA Chamberlin and AUSA Nyhus. In their first meeting on August 3, 2007, Emerson explained how Wu had gained access to Platipus and provided relevant documents.

The same individuals met again on August 30, 2007 and again on March 14, 2008. At the August 2007 meeting, Emerson described what he believed were Hoffman's unethical business practices. At the last meeting, AUSA Nyhus underscored that no cooperation agreement existed between the government and Emerson. Emerson never asserted a Fifth Amendment privilege and provided full information to the government.

In September 2007, Chamberlin questioned Hoffman about his business practices. Hoffman responded to Emerson's allegations that he had not paid the requisite tariffs on products manufactured in China. He subsequently hired someone with experience in customs-related issues who investigated the tariff problem and recommended The Hoffman Group correct past

errors with a payment to U.S. Customs. Hoffman did not remember how much the company paid. Customs never audited The Hoffman Group.

The Hoffman Group obtained default judgments in its Multnomah County case against Wu and Soutavong, but Khoo and Emerson defended the action. Because The Hoffman Group refused to provide requested discovery, the court imposed discovery sanctions against it. As a result, The Hoffman Group offered to dismiss with prejudice Emerson and Khoo. On May 22, 2008, the court issued a judgment and money award to Emerson and Khoo.

The indictment in this case was returned on August 19, 2009. On February 3, 2010, Emerson's attorney, Edelson, advised defendants' counsel, "Mr. Emerson has put this case behind him and is not interested in voluntarily assisting anyone without grant of immunity." Decl. of Christopher Schatz regarding Mot. for Issuance of Third-Party Subpoenas Duces Tecum, Ex. C (#39).

DISCUSSION

The two remaining pending motions are defendants' Motion to Exclude Images of the Wu Laptop and External Hard Drive and defendants' Motion to Compel Government to Extend Use Immunity to Brian Emerson.

I. Motion to Exclude Images of the Wu Laptop and External Hard Drive (#34)

Defendants seek to exclude the two images the FBI took from Wu's computer hard drive: the Acronis Backup Image and the Laptop Image. Defendants contend that neither the Acronis Backup Image nor the Laptop Image are accurate copies of Wu's computer before it was seized. As a result, defendants seek to exclude the images under Federal Rule of Evidence 901 (lack of authentication), Federal Rule of Evidence 1002 (inadmissible duplicates), or Federal Rule of

Evidence 1003 (substantial questions re: authenticity require exclusion). The government clarifies in its closing brief that it intends to offer the images as duplicates of what the FBI took into custody, and does not intend to offer the images as proof of what was on Wu's computer before it was taken by Hoffman and Hansen.

I address defendants' arguments as to each Image separately because the Acronis Backup Image and the Laptop Image contain content that is different for the following reasons: the time when the content was captured, the technology used, and the extent to which the original was accessed before the images were made.

A. Legal Standards Related to Federal Rule of Evidence 901

"The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). The burden on the proponent is not heavy; it needs to make a prima facie showing of authenticity. The burden is met when "sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity." United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000).[2] Under Federal Rule of Evidence 901(a), once the proponent of the evidence makes a prima facie showing of authenticity, the probative strength of the evidence is for the jury. Id.

If the evidence is connected with the commission of a crime, the government must "also establish a connection between the proffered evidence and the defendant," id., and "establish the

[2]Defendants advocate a burden of clear and convincing, but I am unwilling to impose a heightened burden without case law specific to the technology at issue here. See United States v. King, 587 F.2d 956, 961 (9th Cir. 1978) (suggesting burden on government to introduce sound recordings is clear and convincing); United States v. Morrison, 153 F.3d 34, 56 (2d Cir. 1998) (the heightened standard relates to audio recordings).

chain of custody." United States v. Harrington, 923 F.2d 1371, 1374 (9th Cir. 1991). With respect to the chain of custody, the prosecution "must introduce sufficient proof so that a reasonable juror could find that the [evidence is] in 'substantially the same condition' as when [it was] seized." Id. (quoting Gallego v. United States, 276 F.2d 914, 917 (9th Cir. 1960)). The court may admit the evidence "if there is a 'reasonable probability the article has not been changed in important respects.'" Id.

1. Acronis Backup Image

The Acronis Backup Image is a copy of the Acronis Backup made by Hansen. Defendants' challenge to the Acronis Backup Image falls into the following categories: Hansen could have changed the data prior to making the Acronis Backup; the Acronis software that made the Backup is not a forensic tool and did not capture all the data on the laptop; and the FBI failed to follow standard practices in making an image of the Acronis Backup.

a. The Government's Use as Proof of What it Took Into Custody

As an initial matter, the government clarified in its closing brief that it intends to offer the image as a duplicate of what the FBI took into custody, and does not intend to offer the image as proof of what was on Wu's computer before it was taken by Hoffman and Hansen. All but one of defendants' arguments go to the integrity of the Acronis Backup, not the integrity of the Acronis Backup *Image*. Defendants only argument questioning the integrity of the Acronis Backup *Image* has to do with the FBI's alleged failure to follow standard procedures. As I discuss below, at least at this point I reject the defendants' assertion that the FBI's actions warrant exclusion of the evidence. Accordingly, while I question the attenuated connection of such evidence to the defendants' charged conduct, I conclude at this point that the government

has met its prima facie burden that the evidence is what it is purported to be. The Acronis Backup Image will be admitted as evidence of what the government obtained, if the government is able to show its relevancy.

b. The Government's Use as Proof of the Contents of Wu's Computer

Even if, as the defendants expect, the government intends to argue that the Acronis Backup Image contains some of the content that was on Wu's computer prior to Hoffman's seizure of the laptop, I would find the government has met its prima facie burden so long as the government presents the evidence in an appropriate fashion.

Defendants contend that computer data can be changed or deleted, and a savvy computer user can cover up such work. Defendants hypothesize that "Hansen and Hoffman could have uploaded incriminating information onto Wu's computer, altered the dates associated with that information's uploading, installed Acronis to overwrite the data associated with that change, and then made a selective digital image of the hard drive to turn over to the FBI." Khoo's Mem. of Points and Authorities in Supp. of Mot. to Exclude Images 15-16.

There is no evidence, however, that Hansen had the desire or inclination to change the contents of the hard drive before he created the Acronis Backup and, while Hoffman may have had both the desire and the inclination, Hoffman was not in the room at the time Hansen made the Backup. Additionally, there is no evidence or allegation that anyone accessed the Acronis Backup after Hansen made it, until the FBI made an image of it. "The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility." United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988); United States v.

Safavian, 435 F. Supp. 2d 36, 39-40 (D.D.C. 2006) ("The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents).") (emphasis in original).

Defendants' second objection is that the Acronis software failed to capture all the data on the laptop. To understand this argument, some explanation of the Acronis software is necessary. As defendants' expert Bean explained, "Acronis was designed as an archival tool that, once installed on a target computer, allows a user to selectively choose data from that computer to copy on a file-by-file basis." Decl. of Michael Bean in Supp. of Mot. to Exclude Images ¶ 5. As a result, Acronis captures data on the "logical" level, as opposed to the "physical" level. Id. This means it does not capture unallocated space, which is the space holding deleted files and documents until new installations occupy that space. Furthermore, the Acronis Backup Image does not contain the systems files allowing for data and registry analysis and the software is not capable of capturing the "hash value" of the file. The "hash value" is a series of numbers that acts as a digital fingerprint; when the hash value changes it means the content of a file has changed. The government does not dispute this characterization of the Acronis software.

Defendants argue that due to the inherent weaknesses of the Acronis software, the government is unable to show that the Acronis Backup Image is an authentic copy of the Wu laptop before it was seized. It did not "accurately reproduce[] the entirety of the electronic data that existed on the Wu laptop prior to its seizure." Defs.' Mem. of Arg. re: Mot. to Exclude Images 28. They rely on Bean's testimony that application of the Acronis software by Hansen provided "basically a snapshot in time for those specific files" and did not copy the computer "at

what is known as a 'physical' level, producing a bit-for-bit copy known as a 'forensic image.'" Tr. 153; Bean Decl. ¶5. As a result, Bean did not believe the Acronis Backup Image captured the data that was on the Wu computer prior to its seizure because it did not capture the unallocated space. Tr. 133.

There is no question that Acronis is not a forensic tool. Indeed, the government's witness, Portland Police Officer Johns, agreed that Acronis is not a standard forensic imaging tool. Tr. 164. Consequently, defendants are correct that the government may not argue that the Acronis Backup Image "accurately reproduced the entirety of the electronic data" on the laptop. The government is in control of how it uses the evidence, however. Thus, while the government may not argue the Acronis Backup Impage is a reproduction of all the data on the laptop, it may argue that the Acronis software produced an accurate "snapshot" of those files it did capture.

As for the absence of dates of creation of the documents on the Acronis Backup Image, the fact that the Acronis Backup (and therefore the Acronis Backup Image) did not capture the "hash values," defendants may argue to the jury that the evidence is not the same as the content on the laptop seized from Wu on October 17, 2006. Defendants may make a similar argument with respect to the failure of the software to capture unallocated space. "[O]nce adequate foundational showings of authenticity and relevancy have been made, the issue of completeness then bears on the Government's burden of proof and is an issue for the jury to resolve." United States v. Soulard, 730 F.2d 1292, 1298 (9th Cir. 1984). I find with a reasonable likelihood that there was no material change in the evidence between Hansen capturing it on the Acronis Backup and the time when it came into the FBI's possession.

Finally, defendants contend the FBI neglected to follow standard industry practice when they made the Acronis Backup Image. Most obviously, the Acronis Backup Image has a creation date of October 3, 2006, even though the FBI did not have the Acronis Backup until October 20, 2006. The FBI was utterly unaware of this discrepancy, but any error in the creation date goes to the weight of the evidence, not its admissibility. See United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) (alleged inaccuracy of computer printouts went to weight, not admissibility).[3] With respect to the failure to follow other standard protocols, defendants have not identified any harm caused by the protocol the FBI used in making the Acronis Backup Image.

The government has met its low burden that the Acronis Backup Image is a copy of what the FBI received when it took custody of the Acronis Backup. Furthermore, the Acronis Backup Image is a copy of a portion of the contents of Wu's laptop computer on the day it was seized from him. If the evidence is relevant, and the government introduces it with appropriate testimony or circumstantial evidence,[4] the Acronis Backup Image will be received.

2. Laptop Image

---

[3]Unless defendants are able to present new evidence upon obtaining the FBI's protocols, the Court views as reliable the opinions of SA Slinkard and Officer Johns that the FBI followed standard protocols as to the method used to create the Acronis Backup Image. Additionally, contrary to defendants' argument, SA Slinkard testified that he checked the laptop and Acronis Backup into the evidence system when he received them on October 20 and provided them to the NWRCFL at a later date. SA Chamberlin testified that they were checked into the NWRCFL on November 1. There is no unexplained break in the chain of custody once the FBI took custody of the evidence.

[4]Documents may be authenticated by the "testimony of a witness with knowledge" (such as Hansen) or based on the "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Fed. R. Evid. 901(b)(1) and (4).

Again, as I set forth above, the government contends that it intends to offer the Laptop Image as a duplicate of what the FBI took into custody, and does not intend to offer it as proof of what was on Wu's computer before it was taken by Hoffman and Hansen. Given the substantial questions defendants have raised about Hoffman's interference with the contents of the laptop, as I discuss in detail below, I emphasize that I am concerned about whether the evidence is relevant. Nevertheless, the government is the master of its evidence and may, "by deciding what [it] offers it to prove, . . . control what will be required to satisfy the authentication requirement." 31 Charles Alan Wright & Victor James Gold, Federal Practice and Procedure: Evidence §7104 (2000). As with the Acronis Backup Image, the only question defendants raised with respect to the propriety of the FBI's actions was whether the FBI followed standard protocol. Just as with the Acronis Backup Image, at least at this point, I do not find any failure to follow protocol undermined the integrity of the Laptop Image and, in any event, any error will go to the weight of the evidence. The government has met its prima facie burden that the evidence is what it is purported to be–a copy of what the FBI received from Hoffman–and the Laptop Image will be admitted if the government is able to show its relevancy.

However, I conclude that the Laptop Image may not be offered as evidence of what was on Wu's laptop prior to its seizure by Hoffman. In order for the Laptop Image to be admitted into evidence, the government must make a prima facie showing that the Laptop Image is in "substantially the same condition" as the laptop seized from Wu. United States v. Godoy, 528 F.2d 281, 283 (9th Cir. 1975) (per curiam); see also United States v. Dickerson, 873 F.2d 1181, 1185 (9th Cir. 1988) ("Tangible evidence of crime is admissible only when shown to be in substantially the same condition as when the crime was committed."). Furthermore, if there is

evidence of tampering, the government "must show that acceptable precautions were taken to maintain the evidence in its original state." Id.

As an initial matter, Hoffman's history with Wu, including the fact that he had filed a civil lawsuit against Wu the day before he obtained Wu's laptop, raises a question about his motive to change the information on Wu's computer and puts the Laptop Image in a different category from the Acronis Backup Image. Additionally, Hoffman's admitted access to the Wu laptop and his knowledge about computers further supports different treatment of the Laptop Image.

Most importantly, however, the evidence adduced at the hearing supports the notion that Hoffman tampered with the laptop, which resulted in the FBI imaging "bad stuff." Tr. 153. Hoffman himself admitted to booting the computer up and perusing its content over the course of two days. Furthermore, Bean explained that, from his forensic examination of the two Images, between the time the Acronis Backup was made and the time the FBI took possession of the laptop, over 1,000 files or folders were accessed, altered, or deleted. He also found 285 files on the Acronis Backup Image that were absent from the Laptop Image.

Indeed, defendants specifically tasked Bean with examining the Laptop Image to uncover two files named "Hoffman 200601.PST" and "Hoffman2005.PST"(or possibly "Hoffman200502.PST") containing email between Wu and Hoffman, which they represented had been present on the laptop before it was taken. In complying with the assignment, Bean noted there was no indication Wu systematically deleted files created during 2005 and 2006. He commented on several oddities he found, however. First, the Laptop Image contained only one file recorded as deleted that he could recover. Yet, he opined, "[A]s an experienced forensic

computer examiner I expect to find deleted files that are recoverable from unallocated space on the hard drive. The absence of deleted files detectable by forensic software as being recoverable leads me to believe with reasonable forensic certainty that, before the FBI imaged the hard drive, the Wu Laptop hard drive had been altered." Supp. Bean Decl. ¶ 5. Moreover, he found "[t]he unallocated space contained what appeared to be deleted data in some areas but it also contained large blocks of blank or empty space which is consistent with specific targeted wiping or intentional defragmentation of the hard drive." Id. ¶ 6. Based on his review, Bean believed the defragmentation process occurred on October 18 at 11:44 a.m. (China time), which was after Hansen had made the Acronis Backup. Despite the defragmentation process, Bean recovered 17,000 items that had been deleted, one of which was an Outlook file entitled "Hoffman 200601." The file, however, was corrupted. Bean then opined it was reasonable to conclude that the files had existed but had been deleted and overwritten.

Not only did defendants submit evidence that Hoffman accessed the laptop, deleted or changed content, and ran the defragmentation utility, but they raised issues with the way Hansen unknowingly affected the integrity of the laptop. Bean testified that Hansen's action in turning the computer on, moving the private folder to the desktop (thereby altering the Master File Table and displacing deleted content) and installing the Acronis software (thereby replacing content in unallocated space that could have been captured by the FBI's imaging technology) altered the "contents and data configuration of Wu's hard drive." Bean Decl. at ¶6. In short, Bean testified, "There is no way that the data that resides in that [Laptop] [I]mage today is the same as it was when it was surrendered by Wu." Tr. 134.

The government argues that problems with the chain of custody go to the weight of the evidence, not its admissibility. Federal Rule of Evidence 901(a), however, requires the government to "eliminate[] . . . not absolutely, but as a matter of reasonable probability[,]" "[t]he possibility of misidentification and adulteration[.]" United States v. Allen, 106 F.3d 695, 700 (6th Cir. 1997). Here, given Bean's unrebutted expert testimony, I cannot say that the Laptop Image is in "substantially the same condition as when the crime was committed." Dickerson, 873 F.2d at 1185. As the Ninth Circuit explained, "It is of the utmost importance that, so far as practicalities permit, there should not be a legitimate question about the integrity of physical evidence seized by the government and introduced into evidence against an accused." Godoy, 528 F.2d at 284. As a result, the government has failed to meet its burden under Federal Rule of Evidence 901(a) of showing the Laptop Image is authentic because it has not demonstrated it is in "substantially the same condition as when the crime was committed." Dickerson, 873 F.2d at 1185.

B. Legal Standards Related to Federal Rules of Evidence 1002 and 1003

As I set forth above, I found the government met its burden on authenticity with respect to the Acronis Backup Image. Defendants separately argue it should be excluded under the "best evidence" rule. Since I have already concluded that the Laptop Image is not admissible evidence to show what was on Wu's laptop when it was seized by Hoffman, I need only address defendants' argument with respect to the Acronis Backup Image.

Federal Rule of Evidence 1002, the "best evidence rule," provides that: "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." Federal Rule of

Evidence 1003, in turn, provides: "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Federal Rule of Evidence 1001(4) defines a "duplicate" to mean "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original."

Defendants argue the Acronis Backup Image is meant to be a duplication of the original computer, but the government cannot meet its burden of showing that it meets the criteria. The experts on both sides agree that Acronis is not a forensic tool. The failure of Acronis lies in the fact that it permitted Hansen to capture the data he chose to copy, whereas the FBI's Forensic Tool Kit is capable of producing an identical image of an entire hard drive. While the Acronis Backup Image may not be an exact duplicate of the Wu computer, or a "mirror" image, there is no argument or evidence that it is not an exact duplicate of what Hanson chose to copy. Thus, the data captured on the Acronis Backup Image is the "best evidence" of that data. It is not "unfair" to admit this evidence because the Acronis Backup Image is an authentic duplicate of what is on it. It is not a duplicate of the entire computer, but defendants have not shown that the "most critical part of the original . . . is not completely reproduced in the 'duplicate.'" Amoco Prod. Co. v. United States, 619 F.2d 1383, 1391 (10th Cir. 1980).[5] I reject defendants' best evidence objection.

---

[5]Defendants have not produced evidence that the government was aware Hoffman intended to seize Wu's computer. I need not address defendants' spoliation argument.

C. Summary of Rulings on Motion to Exclude Images

In sum, I deny defendants' motion with respect to the Acronis Backup Image and the Laptop Image if the government only intends to offer the Images as proof of what it obtained from Hoffman. Further, the Acronis Backup Image may be offered to prove some of the contents of the laptop, if the government introduces it with appropriate testimony or circumstantial evidence to prove its authenticity. The Laptop Image may not be offered to prove the contents of the laptop Wu possessed.

II. Motion to Compel Government to Extend Use Immunity to Brian Emerson (#40)

Defendants contend that the government must choose how to proceed with respect to Brian Emerson (the individual who was not indicted here, but who was a defendant in the civil case). Emerson believes he may be subject to prosecution (the indictment is open-ended), precluding him from offering favorable testimony on defendants' behalf. Defendants assert the government must: (1) extend use immunity to Emerson; (2) dismiss the indictment; or (3) prohibit the use of any evidence that might otherwise have been clarified, questioned, or rebutted by Emerson.

Defendants concede they must meet a two-pronged test to warrant an order compelling use immunity. First the witness must possess relevant information. United States v. Straub, 538 F.3d 1147, 1157 (9th Cir. 2008). Second, the defendant must show that "the prosecution granted immunity to a government witness in order to obtain that witness's testimony, but denied immunity to a defense witness whose testimony would have directly contradicted that of the government witness, with the effect of so distorting the fact-finding process that the defendant was denied his due process right to a fundamentally fair trial." Id. at 1162.

With regard to the first prong, the government does not appear to dispute that Emerson can provide relevant evidence.

The parties differ, however, in their interpretations of the second prong. Defendants read Straub to allow an order for immunity when the government has "stacked the deck against the defendant in a way that . . . severely distort[s] the fact-finding process at trial." Id. at 1160. Defendants suggest the holding can be read to compel immunity "[w]hen the government has so structured its case that a witness, who would otherwise play a key role in the provision of relevant, exculpatory evidence, does not do so for fear of prosecution[.]" Khoo's Mem. at 12. They call the differences between the cases "superficial" and suggest that the court is not "cabined by rigid requirements[.]" Id. Defendants contend the government has effectively prevented Emerson from sharing what he knows and that Emerson will undoubtedly invoke his privilege against self-incrimination. Hoffman, however, who is central to the government's case, will be able to testify at defendants' trial without fear of prosecution despite engaging in tariff fraud.

The government responds that nothing indicates Emerson is unavailable to defendants or that the information Emerson provided is not otherwise available to defendants. Additionally, it reads the Straub case very closely and points out that of the twelve witnesses the government intended to call, eleven of them had received some level of immunity. As a result, the court found the government "acted with a certain purpose merely by demonstrating that the prosecution committed a set of acts (the selective denial of use immunity described) that had the effect of distorting the fact-finding process." Straub, 538 F.3d at 1157.

Defendants' reading of Straub goes beyond its holding. In evaluating whether I should compel immunity, my scope of review is very narrow. The question comes down to whether the government is exercising its power in a way that "denies the defendant the due process guaranteed by the Fifth Amendment." Straub, 538 F.3d at 1156 (quoting United States v. Alessio, 528 F.2d 1079, 1081-82 (9th Cir. 1976)). Given the Ninth Circuit's "hesitan[cy]" in expanding a Court's authority in this context, I am loathe to accept defendant's view of Straub. Id. at 1160.

Here, the government has not granted selective immunity to any government witness. Hoffman will not testify without fear of incriminating himself–the government has not given him immunity or any similar arrangement. At this point, I see no selective treatment of Hoffman not to prosecute him for tariff fraud; Hoffman has rectified any failure to pay tariffs. Any issues defendants have are more properly the subject of cross-examination. Finally, defendants have access to documentary evidence through the use of Rule 17(c) subpoenas and I have set the trial for a time after the statute of limitations has run against Emerson.

CONCLUSION

For the foregoing reasons, I grant in part and deny in part defendants' Motion to Exclude Images of the Wu Laptop and External Hard Drive (#34) and deny defendants' Motion to Compel Government to Extend Use Immunity to Brian Emerson (#40).

IT IS SO ORDERED.

Dated this 1st day of March, 2011.

/s/ Garr M. King
Garr M. King
United States District Judge