



**TULLY & WEISS**  
RETIRED

**ATTORNEYS AT LAW**

713 MAIN STREET, MARTINEZ, CA 94553

PHONE: (925) 229-9700 \* FAX: (925) 231-7754

---

**The Government's Use of Altered Evidence and False  
Testimony by FBI Personnel to Secure an Illegal  
Conviction in *United States v. Ranieri* (E.D.N.Y. 2019)  
384 F. Supp. 3d 282**

August 31, 2022

---

Exhibit A in support of Motion to Hold Appeal in Abeyance to address New Evidence of Substantive Due Process Violations at Trial in *United States v. Ranieri* (E.D.N.Y. 2019) 384 F. Supp. 3d 282. **Filed September 6, 2022.**

**The Government’s Use of Altered Evidence and False Testimony by FBI Personnel to Secure an Illegal Conviction in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282**

**TABLE OF CONTENTS**

**INTRODUCTION ..... 4**

**I. Anomalies with the FBI Search and Evidence Handling..... 5**

**II. Anomalies with the Evidence Collection, Storage, and Analysis ..... 9**

**III. Anomalies on Hard Drive ..... 13**

**A. The Backup Itself ..... 13**

**B. Folders and Subfolders ..... 14**

**C. Files Within “Studies” Folder ..... 16**

**1. Metadata Regarding Daylight Savings Time Was Manually Altered to Appear As If It Was Automatically Done By A Computer . 17**

**2. Metadata On at Least One Photo Was Falsified to Cover Up That the Photo Had Been Altered..... 19**

**3. Creation Dates Impossibly Precede the Date the Photos Were Taken. The Creation Dates Also Impossibly Precede the Date of the Backup ..... 21**

**IV. Anomalies on Camera Card..... 25**

**A. The Camera Card Was Altered on September 19, 2018, While in FBI Custody ..... 26**

**B. The Camera Card Was Most Likely Altered Between April 11, 2019, and June 11, 2019, While in FBI Custody..... 26**

**1. SFE Booth ’s Second Examination of the Camera Card on June 11, 2019, Was Conducted Under Highly Suspicious Circumstances. 27**

**2. Thirty-Seven New Files Appear to Have Been Added to the Camera Card Between April 11, 2019, and June 11, 2019, While It Was in FBI Custody ..... 28**

**3. The Placement of The Thirty-Seven New Files Indicates That They Were Placed There Manually Rather Than as A Result of Someone Taking Photos ..... 30**

**4. Photo Files IMG\_0093, 94, 96, and 97 Are Bogus..... 34**

**5. Telltale Missing Data from SFE Booth ’s June 11, 2019, Camera Card Report ..... 34**

**V. Anomalies in the Alignment Between the Camera Card and the Hard Drive ..... 35**

**A. The Thirty-One New Photo Files from SFE Booth ’s June 11, 2019, Forensic Examination that ‘Match’ Photos Files on the Hard Drive Do Not Actually Match..... 35**

**B. No Remnants of the Alleged Contraband Photos Were Found on the Camera Card ..... 35**

**VI. Perjury by Brian SFE Booth, Senior Forensic Examiner for the FBI  
36**

**A. SFE Booth Committed Perjury in Testifying that EXIF Data Was Difficult to Change..... 36**

**B. SFE Booth Committed Perjury in Testifying that It Was Not Unusual to Received Evidence that is Unsealed with No Record of the Unsealing ..... 37**

**C. SFE Booth Committed Perjury in Testifying that There Was No Need to Create a Chain-of-Custody Log Every Time an Evidence Item Is Opened..... 37**

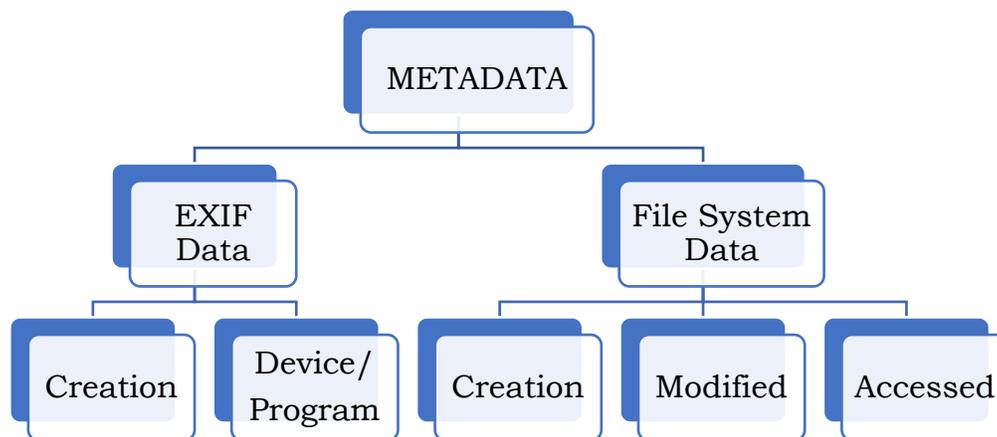
**VII. Prosecutorial Anomalies..... 38**

**The Government’s use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

**INTRODUCTION**

During the jury trial in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282<sup>1</sup>, government prosecutors charged Mr. Raniere, in part with racketeering acts of possession of child pornography and sexual exploitation of a child by using 22 nude photos found on a backup hard drive<sup>2</sup> of a female, identified at trial as “Camila.”<sup>3</sup> The government alleged that the photos were taken when Camila was fifteen. However, by only visually looking at the photos it was not self-evident that Camila was underage at the time the photos were taken, and Camila did not testify. Therefore, the government had to rely on digital evidence and argue two things: one, that the 22 photos were indeed taken at a time when Camila was under 18, and two, the photos were taken by Keith Raniere.

To show Camila was under the age of eighteen in the photos, the government used various metadata, primarily the Exchangeable Image File Format, hereafter “EXIF,” Creation dates of the 22 alleged contraband photos. EXIF Creation dates are ‘birthdays’ of digital photos, assigned to them by the digital camera when the photos are taken.<sup>4</sup> Other metadata can include File System dates, such as “Creation,” “Modified,” and “Accessed” dates, also assigned by the digital camera when the photos are taken. In trial, the government argued that the metadata for the 22 photos showed that they were taken in 2005, when Camila would have been 15 years old and, **because metadata and EXIF data cannot be easily modified**, Camila was underage in the photos.



**Figure A.** *Hierarchy of Metadata types.*

To tie the 22 photos on the backup hard drive to Mr. Raniere, the government could not use the hard drive alone. The hard drive was an external hard drive

<sup>1</sup> Citations to documents in the court record are cited herein as *United States v. Raniere* and or *Raniere, supra*, 18-cr-204-1 (NGG) (VMS).

<sup>2</sup> Referred to as the “Western Digital ‘Hard’ Disc ‘Drive,’” or “WD HDD” at the trial.

<sup>3</sup> See *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 430 – Superseding Indictment.

<sup>4</sup> *Id.* at Trial Transcript hereafter, “Trial Tr.” at 4817:18-4821: 22.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

which supposedly held the backup data of three different computers.<sup>5</sup> Those computers, and the files transferred from them to the hard drive, could have belonged to, or have been used and accessed by several different people within the NXIVM community.

Therefore, the government argued that: (1) Mr. Raniere used a particular Canon digital camera to take the photos; (2) when he took the photos, the camera stored those photos on its camera card<sup>6</sup>; (3) Mr. Raniere then downloaded the 22 photos off the camera card onto a Dell computer; and (4) that computer was backed up to the hard drive.

However, after trial, three top digital forensic experts were hired to analyze evidence relevant to the digital photos. This digital evidence had not been analyzed before or during jury trial due to the government's late disclosure of the evidence to Mr. Raniere's defense team. All three experts, to their surprise and dismay, found a multitude of anomalies that evidenced that the alleged contraband photos were manufactured and planted. The digital evidence had clearly been manually altered to make the photos appear as if they were taken on the specific camera in 2005 before being automatically backed up to the hard drive in 2009.

Further, the folders where the alleged contraband photos were located were created manually but made to look as if they were automatically created by a computer program in 2005. In fact, all the digital anomalies that the experts found on the backup hard drive and the camera card were designed to support the government's narrative which it used to secure convictions for the racketeering acts of possessing child pornography and sexual exploitation of a minor. In the prosecution's own words, these 22 photos were "***the heart of our racketeering conspiracy.***"<sup>7</sup> A summary of the experts' findings follows.

## **I. Anomalies with the FBI Search and Evidence Handling**

Before addressing the technical anomalies that the experts used to prove that the hard drive and camera card were tampered with, it is important to understand the FBI's highly suspicious pattern of activities surrounding these items.

To begin, on March 27, 2018, when the FBI raided 8 Hale Drive, Halfmoon, New York, a residence Mr. Raniere sometimes used, FBI agents entered the home, completely bypassed the entrance, skipped the entirety of the downstairs area, went immediately upstairs, bypassed several more areas, and

---

<sup>5</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4928:3-7.

<sup>6</sup> Referred to as "CF" card, or the camera's compact flash card.

<sup>7</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Status Conference Transcript (March 18, 2019), hereafter "Status Con. Tr." at 19:8-16 [emphasis added].

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

went straight to a study area where, from under a desk, they collected their first two evidentiary items: the Canon digital camera and its camera card. There were several other evidentiary items on top of as well as under the desk right next to the camera that were later seized, but these were not collected initially. The agents then went to a bookshelf on the other side of the same room, and, from the top of this bookshelf, where three hard drives resided side-by-side, they seized the specific backup hard drive in question here.<sup>9</sup>

The FBI then collected eleven more evidence items, some taken from rooms that had been previously skipped over, before returning to look under the same desk from where they had seized the camera. Only in the second search underneath the desk did they collect evidence item #14 - another external hard drive. At the end of the raid, agents returned to the bookshelf and collected the hard drive in question, which was later marked evidence item #2, as well as two other hard drives which were later marked as evidence items #36 and #37. Notably, evidence items #1 and #2, the camera card and hard drive, just so happen to be the only two pieces of digital evidence the government used to argue the child pornography and child exploitation RICO acts, based on an allegedly 'accidental' discovery of the 22 photos nearly ***eleven months later***.

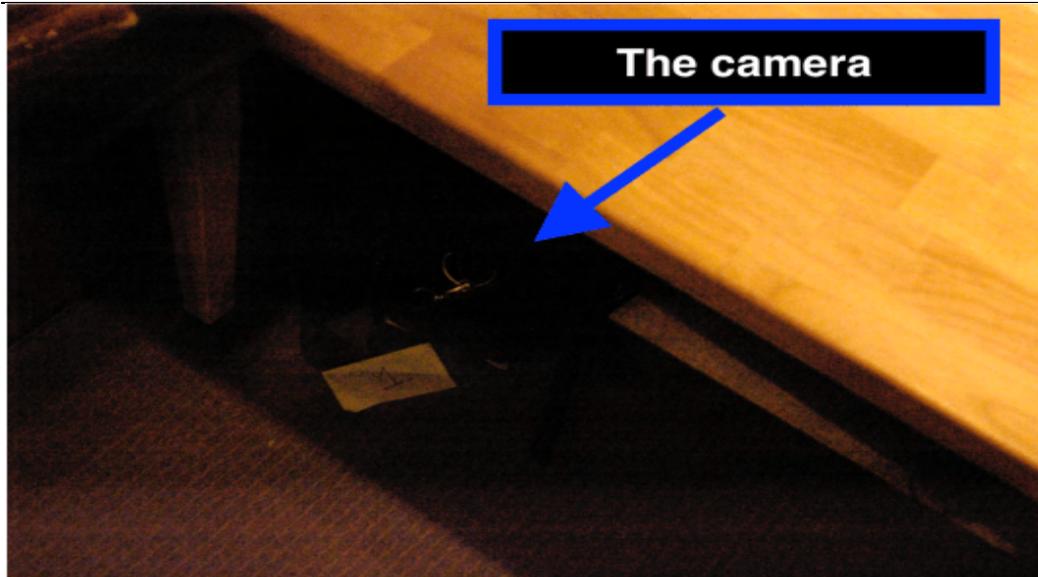


**Figure: B.**<sup>10</sup>

<sup>9</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4297:2-4305:9; Government Trial Exhibit 502A, hereafter "GX 502A," at GX 502A-32 & 33.

<sup>10</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) GX 502A-24.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**



**Figure: C.**<sup>11</sup>

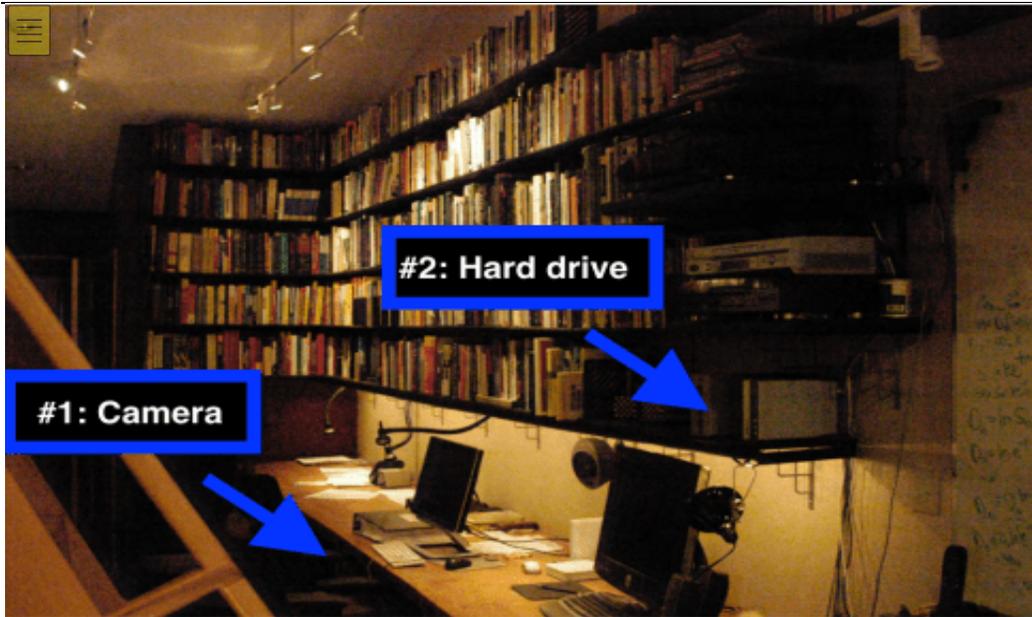


**Figure: D.**<sup>12</sup>

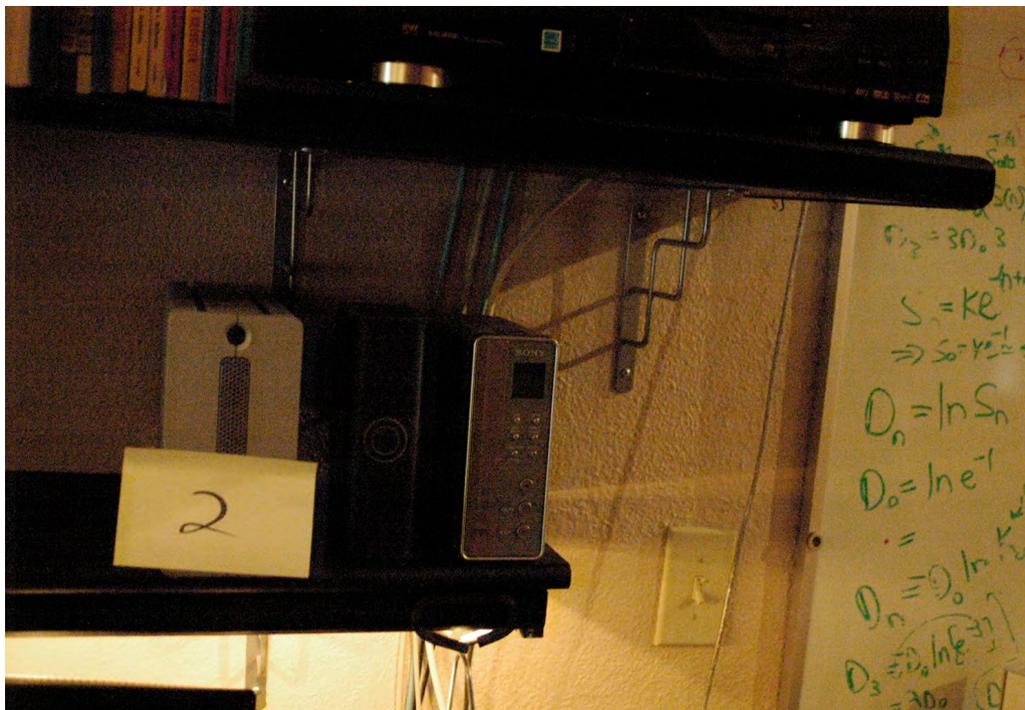
<sup>11</sup> *Id.* at GX 502A-32.

<sup>12</sup> *Raniere*, supra, 18-cr-204-1 (NGG) (VMS) GX 502A-45; see also Trial Tr. at 4304:18-22 [**according to the FBI, evidence was numbered and photographed based on the chronological order of when the evidence was found.**]

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**



**Figure: E.** <sup>13</sup>



**Figure: F** <sup>14</sup> Hard drive containing the 22 photos in the middle of two other hard drives.

<sup>13</sup> *Id.* at GX 502A-24.

<sup>14</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) GX 502A-24.

---

## **II. Anomalies with Evidence Collection, Processing, and Analysis**

The FBI's unusual pattern of evidence collection during the raid on March 27, 2018, belies that at least someone in their party knew these devices would contain alleged contraband photos. The facts surrounding this suspicious pattern of evidence collection stand in stark contrast to the case agent's, FBI Special Agent hereafter "SA," Michael Lever, claim of 'accidental' discovery of the 22 photos on February 21, 2019 – 10 months and 25 days after the hard drive was seized and labeled as "Evidence Item #2."<sup>15</sup> As for the camera and its camera card, despite being the first items seized, SA Lever did not deliver them to the FBI's forensics laboratory, hereafter "CART," for analysis until February 22, 2019 – 332 days after the items were seized.<sup>16</sup>

- On July 10, 2018, SA Maegan Rees checked out the camera and camera card for "evidence review," and returned it July 27, 2018.
- On August 8, 2018, SA Lever delivered the hard drive and other evidence, excluding the camera and camera card, to the CART lab where it was received by Forensic Examiner Trainee Virginia Donnelly, hereafter "FET Donnelly."<sup>23</sup>
- On September 19, 2018, SA Lever checked out the camera and camera card for "evidence review," and returned it September 26, 2018.

In total, SA's Lever and Rees checked out the camera and camera card from evidence control for 24 days for "evidence review." During this time, they had unrestricted access to these critical evidence items. However, FBI protocol **strictly prohibits** case agents from checking out and reviewing data on digital devices before the devices are processed by a forensic examiner in a CART forensic lab.<sup>26</sup> A CART forensic examiner will make a forensic image - an exact copy of a device in the identical state it was in when it was found at the scene - and then will examine the forensic image and not the original device. This protocol preserves the integrity of digital evidence as it keeps the original evidence in a pristine state while still allowing testing on the forensic image.

Both FBI SA's Rees and Lever violated this protocol when they individually checked out the camera and camera card from Evidence Control, for "evidence

---

<sup>15</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 594-2 at ¶ 8 & 11 – Affidavit of FBI Special Agent Michael Lever (Feb. 22, 2019) hereafter "Second Lever Aff." (filed under seal); see also Dkt 618 at 2.

<sup>16</sup> *Id.* at Defense Trial Exhibit 945 hereafter "DX 945," – FBI Evidence Chain of Custody for Item 1; see also GX 502A-32 & 33; Trial Tr. at 4304:16-4305:9.

<sup>20</sup> *Id.* at DX 945.

<sup>21</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. A at 15.

<sup>23</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 001-004.

<sup>26</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. C at 21.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

review” *even though the CART lab had not yet forensically imaged the items.*<sup>27</sup> Thus, they each individually checked out these items for purposes of reviewing them, when FBI protocol specifically prohibits any such review by either of them. Further, it is proven to a scientific certainty that, on September 19, 2018, when SA Lever had the camera and camera card checked out, an unknown person accessed and modified the contents of the camera card at least once.<sup>28</sup>

- On September 19, 2018, FET Donnelly forensically imaged the hard drive.<sup>31</sup>
- On September 24, 2018, FET Donnelly processed the hard drive.<sup>34</sup>
- On September 26, 2018, SA Lever checked the hard drive out of evidence and checked it into storage.
- On October 3, 2018, FET Donnelly notified SA Lever that the hard drive was available through the secure network platform called, “Case Agent Investigative Review” hereafter “CAIR.”<sup>35</sup> Thus, while SA Lever was prohibited from directly analyzing the hard drive,<sup>36</sup> he could look through the forensic image by logging onto CAIR.
- Nonetheless, on February 22, 2019, SA Lever was the last person to accept custody of the hard drive when he checked it out from Evidence Control.<sup>37</sup> There have been no logs which list what SA Lever did with the hard drive. Thus, his actions with it are unknown. It is also unknown who took custody of the hard drive when he was finished with it.

February 22, 2019, is also the date that SA Lever allegedly accidentally ‘discovered’ the 22 alleged contraband photos using the CAIR system. Thus, in addition to being an additional violation of FBI protocol, SA Lever’s physical possession of the hard drive on February 22, 2019, makes no operational sense - he was already accessing a forensic copy of the hard drive on CAIR, he had no need to possess the physical item.

---

<sup>27</sup> *Id.*

<sup>28</sup> *Id.* at Dkt 1169-1 at Ex. D at Bates 006-007 Finding 3; Bates 012 Appendix A; Bates 032 conclusion; Bates 034 Finding 4; Bates 035-036 Finding 3 & 4; Bates 0054 Finding 6.

<sup>31</sup> *Id.* at DX 961 at Bates 011.

<sup>34</sup> *Id.* at DX 961 at Bates 024

<sup>35</sup> *Id.* at DX 961 at Bates 25.

<sup>36</sup> FBI’s Digital Evidence Policy Guide

<sup>37</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Defense Trial Exhibit 960 here after “DX 960,” – FBI Evidence Chain of Custody for Item 2.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

- On February 22, 2019, two hours after he checked out the hard drive,<sup>40</sup> SA Lever delivered the camera card to CART for the first time, turning it over to Senior Forensic Examiner hereafter “SFE,” Stephen Flatley.”<sup>41</sup>
- On April 11, 2019, SFE Brian Booth generated a forensic report for the hard drive based on FET Donnelly's processing.<sup>42</sup> On this same date, SFE Flatley generated a forensic report for the camera card based on his own processing of it.<sup>43</sup>

Importantly, SFE Flatley's report for the camera card when paired with SFE Booth's report for the hard drive, only offered weak support for the government's theory that Mr. Raniere took the 22 alleged contraband photos with the Canon camera then backed those photos up to the hard drive, as there were only four matching photo files between the two devices, 180, 181, 182, and 183.<sup>44</sup>

- On June 7, 2019, SA Lever made an unauthorized<sup>45</sup> request for SFE Booth to reexamine the camera card under the suspect guise of SFE Flatley's unavailability for trial.

SFE Flatley's unavailability arose from a suspicious and sudden reassignment to Ghana, Africa just six days before he would have otherwise been called to testify about the camera card.<sup>46</sup> Moreover, when SA Lever requested SFE Booth to reexamine the camera card, SFE Flatley had had possession of it in the CART lab since February 22, 2019.<sup>47</sup> However, instead of SFE Flatley giving the camera card directly to SFE Booth, who worked in the same CART lab, the items were transferred to SA Elliot McGinnis on June 7, 2019. SA McGinnis had the items in his custody for 3 days before he gave them to SA Christopher Mills, on June 10, 2019. SA Mills had the items in his custody from 10:02

---

<sup>40</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) DX 960 at 3

<sup>41</sup> *Id.* at DX 945 at 3.

<sup>42</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 028.

<sup>43</sup> *Id.* at GX 521A – Forensic Report of the Camera Card by SFE Stephen SFE Flatley (4/11/2019).

<sup>44</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 028, Appendix D, Introduction.

<sup>45</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 037 at Fn. 6 [“The FBI Digital Evidence Policy Guide, Section 3.3.11.2 states, “Unless approved by the AD, OTD as outlined below, examinations are not conducted on any evidence that has been previously subjected to the same type of technical examination (hereinafter referred to as a ‘re-examination.’)” One of the reasons for this policy is to “[e]nsure that the integrity of the evidence is maintained” (p. 37). A publicly released version of this document, which includes many other requirements for a re-examination, may be found at <https://vault.fbi.gov/digital-evidence-policy-guide/digital-evidence-policy-guide-part-01-of-01/view>”].

<sup>46</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4987:1-16; *see also* DX 961 at Bates 029.

<sup>47</sup> *Id.* at DX 945.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

a.m., and then gave them to SFE Booth at 4:55 p.m.<sup>48</sup> On June 11, 2019, during the last week of trial, SFE Booth, *without getting proper authorization*, created a second forensic image, then generated a second forensic report which incredibly showed 37 new files which were not present in SFE Flatley's previous report.<sup>49</sup> This new report, in contrast to SFE Flatley's report, now offered strong support for the government's theory as there were now 31 matching photo files between the two devices.<sup>50</sup>

---

<sup>48</sup> *Id.*

<sup>49</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 029, Appendix D.

<sup>50</sup> *Id.*

The hard drive that contained the 22 photos of alleged child pornography was an external hard drive that had backed up files from three computers. While the government presented the folder containing the 22 photos in trial as part of a normal backup performed from a computer allegedly belonging to Mr. Raniere, the computer was never located. Additionally, forensic examination by experts with extensive law enforcement backgrounds, former FBI Special Agent Dr. J. Richard Kiper, Ph.D.<sup>60</sup> and Steven Abrams, who worked extensively with law enforcement including the United States Secret Service,<sup>61</sup> revealed that the files, folders, and metadata were manufactured and/or altered and manually planted on the hard drive. Thus, the 'child pornography' was manufactured and Mr. Raniere was framed.

### **A. The Backup Itself**

The hard drive appeared as if someone had used it to back up files from three different computers.<sup>62</sup> Two of the backups were typical, but the third was aberrant. The alleged contraband photos were located in the third, aberrant backup.

The two 'typical' backups contained folders commonly used in computer backups such as "My Documents," "Desktop," and "Favorites." While the aberrant backup did contain folders called, "My DVD's," "My Music," "My Pictures," "Studies," and "Symantec," these folders were practically empty. "My DVD's" contained no DVD's, "My Pictures" contained one, sample picture, and "Symantec" contained only traces of a text file. The only two folders with significant content were "Studies," which contained 167 nude photos including the 22 alleged contraband photos and one photo of a tree, and "My Music," which contained 150 or so music files.

The aberrant backup also occurred in a suspicious two steps. In the first step, only the "Studies" folder containing the 22 alleged contraband pictures was backed up. In the second step, performed approximately 90 minutes later, the other folders "My DVDs," "My Music," "My Pictures," "Studies," "NeroVision," and "Symantec" were backed up.<sup>68</sup> Since the folders in this second step were practically empty, it does not make logical sense for anyone to back them up.

Thus, the data here is more consistent with someone planting the "Studies" folder on the hard drive in such a way to make it look like a backup and then,

---

<sup>60</sup> *Id.* at Dkt. 1169-1 at Ex. D, E, F; *see also* Ex. D1. [Dr. J. Richard Kiper, Ph.D., served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics].

<sup>61</sup> *Id.* at Ex. E at Bates 001.

<sup>62</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 010, Finding 7; *see also* Trial Tr. at 4928:3-7.

<sup>68</sup> Dkt. 1169-1 at Ex. D at Bates 010-011, Finding 7.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

90 minutes later, adding the other empty folders and the music files to make the 'backup' appear more legitimate.

**B. Folders and Subfolders**

Within the "Studies" folder were subfolders. The subfolders were named in a YEAR-MM-DD-HHMM-SS format purporting to show the time that the subfolder was created. For instance, "2005-11-02-0422-20," would represent November 2, 2005, at 4:22:20 am.<sup>70</sup> These folders appear to be computer-generated as users do not typically name folders after exact times down to the second.<sup>71</sup>

These particular subfolders will be referred to as "DateTime" folders. The DateTime folder names roughly match the metadata (e.g. the EXIF Creation dates) of the photo files stored within. In other words, these DateTime subfolders present as if the photos they contain were taken in 2005 and that, shortly after being taken, someone downloaded the photo files to the computer using a program that automatically generated these DateTime folders. However, like all folders on a computer, the names of these DateTime folders are easily modifiable. Nonetheless, the government relied upon these DateTime folder names together with metadata of the photo files' within them, which is also easily modifiable, to date the photos to 2005 in arguing its case at trial.<sup>72</sup>

However, anomalies with the DateTime folders show that, while they appear to be the result of automation via computer software, it is scientifically provable that some, if not all, of these folders are rather the result of manual manipulation.<sup>73</sup> Firstly, these subfolders could not have been generated by the Canon camera. That particular Canon camera generates folders named "CANON100" to store the first 100 photos, "CANON200" to store the second 100 photos, "CANON300" to store the third set of 100 photos, and so on. Therefore, any subfolders that were created to contain photos from the Canon camera that do not follow this naming convention were either created through other computer software or manually, not by the camera.<sup>74</sup>

Secondly, in evaluating between computer automation or manual manipulation, there are two anomalies present in these DateTime folders that prove manual manipulation. The first anomaly is that two subfolders, "2005-10-19-0727-57" and "2005-10-19-0727-59," appear to have been created two seconds apart, at 7:27:57 am and 7:27:59 am, respectively, on October 19, 2005. DateTime folder 2005-10-19-0727-57 contained photo files 90-98.

---

<sup>70</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4873:19 – 4874:4.

<sup>71</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 008, Finding 6.

<sup>72</sup> *Id.* at Trial Tr. at 5371:16-24.

<sup>73</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 008-009, Finding 6.

<sup>74</sup> *Id.*

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

DateTime folder 2005-10-19-0727-59 contained photo files 79-89. However, for these times to be authentically created, this would require a user selecting one batch of photo files from the camera, 90-98, choosing an option through a software program to download them to a computer, waiting for them to fully download, and then selecting the second batch of photo files from the camera, 79-89, choosing the option through the software program to download them to a computer, and waiting for them to fully download – all within two seconds. That is implausibly fast. [Maybe use JD's video example here. He will have to do affidavit to establish foundation for the demonstrative evidence.] More plausibly, someone named the folders manually but did not take reality into account.<sup>75</sup>

Thirdly, an anomaly was discovered in what is called a “Thumbs.db” file. In earlier versions of Windows, a Thumbs.db file was automatically generated for each folder and contained previews of each file in that folder. If a person opened a folder and clicked on “icon view” to look at the thumbnail images of the files in that folder, the Thumbs.db file was what allowed this to happen.<sup>76</sup>

As one would expect, there was a “Thumbs.db” file in each of the two subfolders, “2005-10-19-0727-57” and “2005-10-19-0727-59.” However, the Thumbs.db file in both 2005-10-19-0727-57 and 2005-10-19-0727-59 each contained previews of photo files *79 all the way through 98*. This means that all the photos, photo files 79-89 and photo files 90-98, used to reside in a single, originating folder. This means that the entire set of photo files were first downloaded to a computer in one folder before someone manually separated the ranges and put them into the two separate subfolders. If the sets were downloaded to separate folders originally as their names indicate, each Thumbs.db file would only contain thumbnails for their specific set, 90-98 or 79-89, respectively. This further contradicts the “automatic” insinuation of the folder names.<sup>77</sup>

Thus, it is proven to a scientific certainty that subfolders 2005-10-19-0727-57 and 2005-10-19-0727-59 were manually manipulated with the intention of appearing to be automated backups, in exact alignment with the government's narrative. This does not mean that the other subfolders were *not* manipulated, it only means that evidence of tampering in the other subfolders was not yet discovered given the minimal discovery that the Defense has received to date. While these two DateTime subfolders, 57 and 59, were not alleged to contain any contraband photos, they exist on the same hard drive where the alleged contraband photos were ‘accidentally’ discovered by SA Lever and they helped to support the same narrative that the government used to argue the illegal nature of alleged contraband photos.

---

<sup>75</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 008-009, Finding 6.

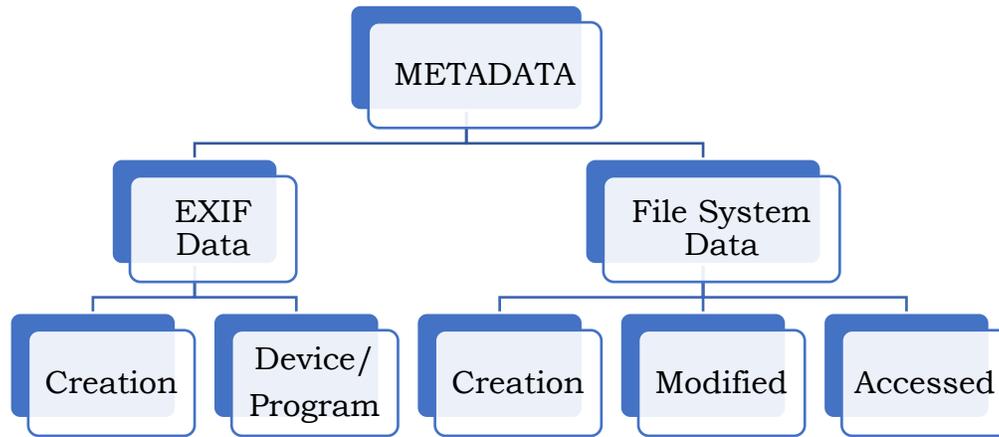
<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

**C. Files Within the “Studies” Folder**

Within the “Studies” folder, photo files’ metadata was manually altered to comport with the government’s narrative that the alleged contraband photographs were taken in 2005.

To understand the tampering done to these files, it is important to understand what an “EXIF Creation” date is and what “File System Creation,” “Modified,” and “Accessed” dates are. It is also important to remember that all EXIF and File System data can be *easily* changed by even an unsophisticated user on a computer.



**Figure A.** *Hierarchy of Metadata types.*

An EXIF Creation date is the date set on a photo by the camera when taken.<sup>78</sup> This date will not change without manual alteration of the data. Even a modification of the image will not change this initial EXIF Creation date. In contrast, a File System, hereafter “FS” Creation date is automatically updated each time the file is saved to a new device.<sup>79</sup> For example, there is an initial FS Creation date when the picture arrives to the camera card. The EXIF Creation date and the first FS Creation date will be almost identical. However, when a photo file is sent to another device, downloaded to a computer, or backed up to a hard drive, the FS Creation date get updated, whereas the EXIF Creation date will not change. However, the FS Creation date will not change if a photo is merely moved from one folder to another, on the same device.

The File System Modified date is the date that marks the last time the photo was edited.<sup>80</sup> The initial FS Modified date will be almost identical to the EXIF Creation date as well. The FS Modified date will not change unless the photograph is modified in some way, such as applying a filter or cropping it.

---

<sup>78</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D. at Bates 007 Finding 4.

<sup>79</sup> *Id.*

<sup>80</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D. at Bates 007 Finding 4.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

The FS Modified date will not automatically change upon transfer to a new device.<sup>81</sup> Thus, even if a photo file is moved from a camera card to a computer, and then to a backup hard drive, if the photo file is not modified from the original picture taken, the FS Modified date will not change. The only exceptions to this are 1.) if the device that the photo file is saved on has a different time zone than a receiving device, or 2.) if the receiving device has a daylight savings setting that is turned on, then the FS Modified date might change on the receiving device to reflect the new time zone or be adjusted by one hour for daylight savings.

The File System Access date is the date that marks the last day the photo file was opened. The photo file need not be modified in any way to have the FS Access date change.

Imagine a puppy born to a school for dogs that trains them to be service animals. When the puppy is born, it would get a birth certificate from the veterinarian and the school would create a document noting the puppy's official acceptance into the school. The birth certificate would be the EXIF Creation date and the acceptance into the school would be the FS Creation date. The dates and times would be very close, if not identical. If the puppy was sent to a different school, that school would create a new document noting the puppy's official acceptance, but this would not affect the puppy's birthdate on its birth certificate. As the puppy is put through different training modules, the school would keep track of the courses the puppy has completed to mark the change in its behavior. Each record of the puppy graduating from a module would be an FS Modified date. Lastly, the school would want one of their staff to periodically see and touch the puppy to give it personal attention such as a play day. This would be the FS Accessed date.

The birth certificate (EXIF Creation date) of the puppy would always stay the same, unless someone tampered with it. However, if the puppy was ever sent to a different school, for every new school the puppy was sent to, it would receive a new acceptance certificate (FS Creation date). For every training module it completed at any school, it would receive a new training certificate (FS Modified date). Every time after birth that the puppy was seen and given personal attention such as a play day, that would be logged as well (FS Accessed date).

**1. Metadata Regarding Daylight Savings Time Was Manually Altered to Appear as If It Was Automatically Done by A Computer**

To understand how the metadata shows tampering, one must keep in mind that, while an EXIF Creation date does not change when a file is copied to another computer, an FS Creation date does. The FS Modified also does not automatically change when a file is copied to another computer, but it *may* be

---

<sup>81</sup> *Id.*

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

interpreted differently when the file is copied, depending on the new computer's time zone settings.<sup>82</sup>

Daylight Savings Time in 2005 occurred on Sunday, October 30, at 2:00 a.m.<sup>83</sup> Photo files 43 to 126 in the "Studies" folder have metadata that insinuate that they were taken *before* the daylight savings change, between October 16, 2005, and October 29, 2005. However, photo files 127 to 149 have metadata insinuating they were taken *after* the daylight savings change on October 30, 2005 after 2:00 a.m.<sup>84</sup>

The photos allegedly taken *before* the daylight savings change, photo files 43 to 126, had FS Modified dates one hour behind those of the EXIF Creation dates.<sup>85</sup> This could naturally occur on a computer *if* the computer was set to compensate for daylight savings time. Imagine a puppy born to a school in Arizona, a state which does not observe daylight savings, that is transferred to a school in California, a state which does observe daylight savings. The a school in California would not change the veterinarian's birth certificate for the puppy, but it may adjust the time of the puppy's Arizona training certificates by one hour to conform to California's observance of daylight savings.

However, for photo files 127 to 137, purportedly taken *after* the October 30, 2005 daylight savings time switch, their FS Modified dates were **two hours** behind the time listed in the EXIF Creation dates.<sup>86</sup> Then, on the same day, for photo files 138 to 149, their FS Modified dates **matched** their EXIF Creation dates.<sup>87</sup> Notably, photo files 127 to 137 belonged to a single folder and were the only photos on the hard drive with this two-hour difference between their EXIF Creation dates and their FS Modified dates. **Nothing outside of human intervention could account for these changes.**<sup>88</sup> This would be akin to the puppy school in California receiving a litter of puppies from Arizona when California was observing daylight savings and adjusting the time of the puppies' Arizona training certificates by two hours for the first half of the litter and then by zero hours for the second half. While humans may make these mistakes, computers cannot.

---

<sup>82</sup> *Id.*

<sup>83</sup> Clock Changes in New York, New York, USA 2005 (Accessed on August 28, 2022) found at <https://www.timeanddate.com/time/change/usa/new-york?year=2005>

<sup>84</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Appendix B, at Bates 015 - 019.

<sup>85</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

<sup>86</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

<sup>87</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

<sup>88</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

Further, here, neither the Canon camera nor the camera card are able to store a time zone.<sup>89</sup> Therefore, it is not possible that a computer receiving these photo files would automatically adjust the FS Modified dates for the time zone. It is unlikely but not impossible that the computer could automatically adjust the FS Modified date by one hour for daylight savings,<sup>90</sup> akin to the puppy school in California routinely adjusting the time of a puppy's initial acceptance that it received from *any* outside school by one hour, *just to be sure that*, if there was a daylight savings adjustment, that adjustment would be guaranteed. This is possible, but highly unlikely.

Regardless, what is ironclad is that the **two-hour** difference could not have come from an automatic adjustment by a computer since Daylight Savings Time only adjusts by one hour. Also, the inconsistency between photo files 127 to 137 being adjusted (two hours) and photo files 138 to 149 not being adjusted at all (zero hours) is a scientific impossibility; either the computer is set to adjust for daylight savings for photo files with EXIF Creation dates after October 30, 2005, at 2:00 a.m. or it is not. Because all photo files in 127 to 149 present as being taken *after* the daylight savings change, either they all should have been adjusted, or none should have been adjusted.

Since computers cannot have made these mistakes, manual intervention is the only explanation here. Thus, it can be concluded that the dates of the photos in the "Studies" folder were manually manipulated as human tampering is the most plausible explanation for these otherwise inexplicable anomalies.

**2. Metadata On at Least One Photo Was Falsified to Cover Up That the Photo Had Been Altered**

Adobe Photoshop Elements is a popular consumer photo-editing program. It is a sister product to Adobe Photoshop, a more well-known professional photo-editing program. Like all such photo-editing programs, if someone used Adobe Photoshop Elements to edit a photo file, the program would leave a mark in the photo file's EXIF data. Specifically, the photo file's EXIF CreatorTool value would get set to "Adobe Photoshop Elements." This lets someone looking at the EXIF data know what program was used to modify the photo file. **Kiper Ex. D, Finding 5, bates 7-8.**

The alleged contraband photos on the hard drive are photo files 150 to 163 and 184 to 191.<sup>92</sup> Photo file 175 appears in the middle of these two ranges. Like the

---

<sup>89</sup> Canon EOS 20D Digital Camera Manual at 34 (setting the date and time), found at <http://gdip01.c-wss.com/gds/9/0900000259/01/EOS20DIM-EN.pdf>

<sup>90</sup> The Windows Club – Adjusting For Daylight Savings Time Automatically, found at <https://www.thewindowsclub.com/enable-or-disable-adjust-for-daylight-saving-time#:~:text=automatically%20toggle%20button,-.Windows%2010,saving%20time%20automatically%20toggle%20button>

<sup>92</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4875:24 - 4879:4.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

other photo files on the hard drive, photo file 175 contains in its EXIF data the model and serial number of the Canon camera. **However, its EXIF CreatorTool value is set to “Adobe Photoshop Elements 3.0,” evidencing that Adobe Photoshop was used to open and modify the photo file’s data.**<sup>93</sup> The “Adobe Photoshop Elements 3.0” CreatorTool value is not present in the EXIF data of any of the other photo files in the “Studies” folder.<sup>94</sup>

The “Adobe Photoshop Elements 3.0” CreatorTool value could not have been put on photo file 175 by the Canon camera. Adobe Photoshop is a computer program that only runs on a computer, not a camera. Therefore, the “Adobe Photoshop Elements 3.0” CreatorTool value had to be put inside the EXIF data of photo file 175 **by a person running the Adobe Photoshop Elements program on a computer and editing that photo file.**

Though it cannot be discerned just how, we do have definitive proof that someone did indeed tamper with at least photo file 175 because its metadata was manually altered to cover up that the file had been changed. The proof of this is shown by comparing the two alleged counterparts for photo file 175 on the camera card, where it purportedly originated, versus its copy on the hard drive, where it was purportedly backed up. On the camera card, the FS Modified date for photo file 175 is November 10, 2005, at 8:25:04 p.m. On the hard drive, the FS Modified date for photo file 175 is November 10, 2005, at 8:25:04 p.m. Thus, they appear to be identical. However, we know that photo file 175 on the hard drive was modified on a computer *at some point* using Adobe Photoshop Elements because its CreatorTool value was set to “Adobe Photoshop Elements 3.0” whereas the photo file on the camera card was not. **Kiper Ex. D, Finding 5, bates 7-8.**

Therefore, because photo file 175 on the hard drive *was* modified on a computer *at some point* using Adobe Photoshop Elements, the FS Modified date for photo file 175 on the hard drive *should be different* than its alleged counterpart on the camera card, which did not have its CreatorTool value set to “Adobe Photoshop Elements 3.0.”<sup>95</sup> However, inexplicably, their FS Modified dates are the identical, down to the exact second. Thus, we can say to a scientific certainty that someone manually altered photo file 175’s FS Modified date on the hard drive to make it appear as if the photo had not been modified, when in fact it had. Further, the fact that only one file on the hard drive, photo file 175, contains the EXIF CreatorTool value set at “Photoshop Adobe Elements 3.0” is likely due to an oversight on the part of the person altering the EXIF data. **It is likely that other photos in the “Studies” folder had also been altered using Adobe Photoshop Elements but the EXIF data regarding the CreatorTool was manually changed to set the value at zero to cover up the**

---

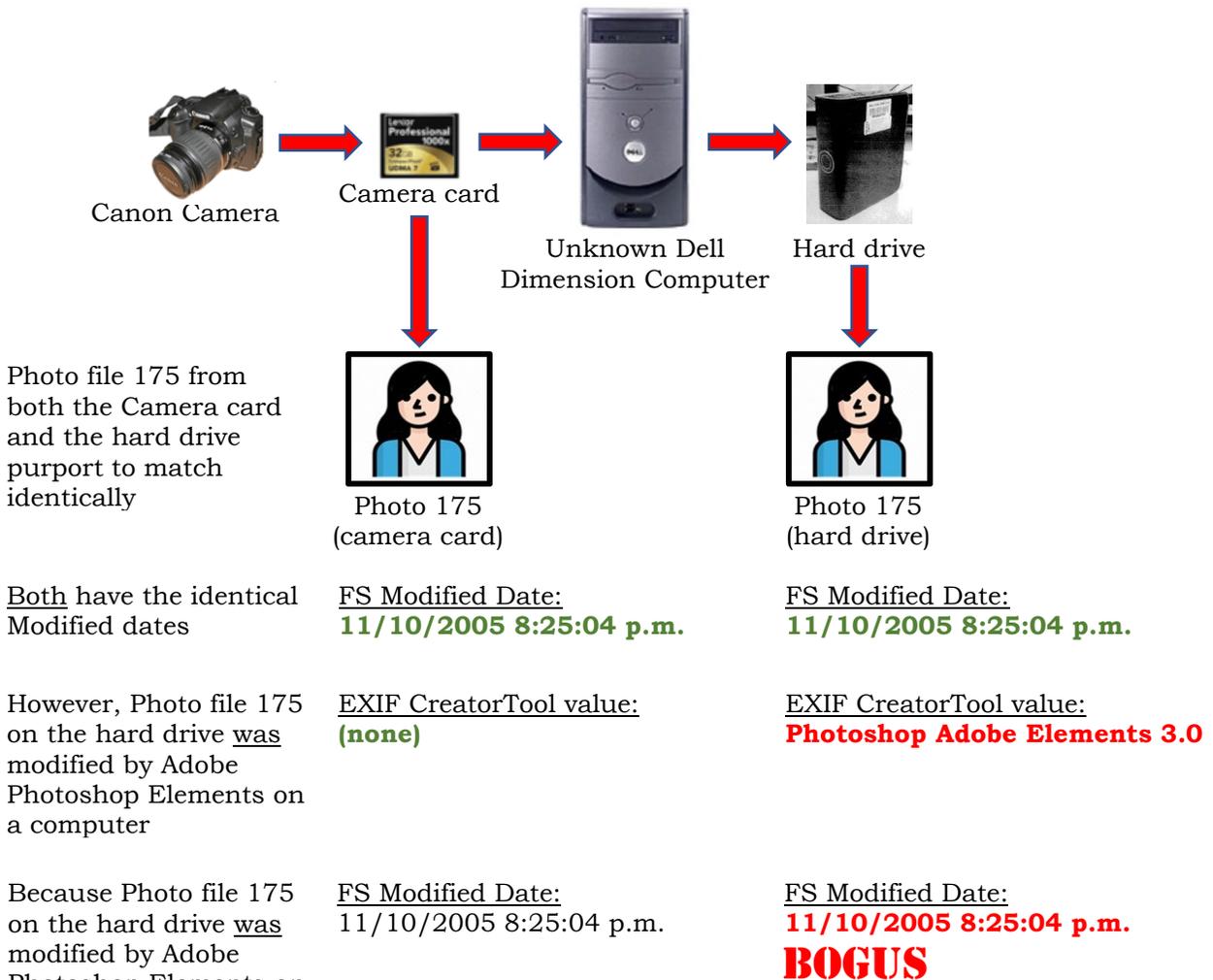
<sup>93</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 007-008, Finding 5.

<sup>94</sup> *Id.*

<sup>95</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007-008, Finding 5.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniero* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

alterations and the tamperer(s) merely made the mistake of leaving the EXIF CreatorTool value for photo file 175 set at "Photoshop Adobe Elements 3.0."<sup>96</sup>



**Figure G:** Photo file 175 was altered on a computer but someone tried to cover that alteration up.

**3. File System Creation Dates Impossibly Precede Both the Date the Photos Were Allegedly Taken and the Date the Photos Were Allegedly Backed Up.**

<sup>96</sup> *Id.*

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

When a file is copied to another device, the FS Creation date for the file automatically updates upon transfer, marking when the file was copied to the new device. When a folder containing files is copied to another device, the FS Creation date for the folder, *and all of the files within it*, are automatically updated, marking when the folder, and all of the files within it, were copied to the new device. Further, FS Creation dates are updated to the current clock time of the computer receiving the files; if one copied photo files with FS Creation dates of January 1, 2019, from one computer to another on January 1, 2022, the moved photo files would receive a new FS Creation date of January 1, 2022, updated from January 1, 2019.

FS Creation dates are also updated when files are backed up from a computer to a backup hard drive. However, because a backup hard drive does not have its own clock like a computer does, the FS Creation dates for the backed-up files would adopt whatever time the computer's clock was set to *at the time of the backup*. For instance, if one set the clock back on their computer from January 1, 2022, to January 1, 2019, nothing would happen to the files on the computer. However, if one then backed up files to a hard drive, because the hard drive does not have a clock of its own, the files would adopt their FS Creation dates from the transferring computer *at the time of the backup*. Thus, in this example, the files backed up to the backup hard drive would have FS Creation dates of January 1, 2019.

However, while FS Creation dates automatically change every time a photo is copied to another device, be it another computer or backup hard drive, neither the EXIF Creation date nor the FS Modified date automatically change. The EXIF Creation date will not change unless it is manually altered. The FS Modified date will not change unless the photo is edited, the data is manually altered, or it is automatically adjusted based on a time zone setting.

Thus, on a computer, FS Creation dates should be the *same as* or *come after* the EXIF Creation and FS Modified dates. In an automatic computer backup, FS Creation dates should *always come after* the EXIF Creation and FS Modified dates, since the backed-up files will get updated FS Creation dates, while the EXIF Creation and FS Modified dates will not. **Kiper finding 7, Bates 10-11.**

**The Government’s use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

<p><b><u>Photo taken January 1, 2022</u></b></p> 	<p><b><u>FS Creation Date</u></b> January 1, 2022</p>	<p><b><u>EXIF Creation &amp; FS Modified Date</u></b> January 1, 2022</p>
<p><b><u>Same photo moved to computer February 1, 2022</u></b></p> 	<p><b><u>FS Creation Date</u></b> February 1, 2022</p>	<p><b><u>EXIF Creation &amp; FS Modified Date</u></b> January 1, 2022</p>
<p><b><u>Same photo backed up to hard drive on March 1, 2022</u></b></p> 	<p><b><u>FS Creation Date</u></b> March 1, 2022</p>	<p><b><u>EXIF Creation &amp; FS Modified Date</u></b> January 1, 2022</p>

**Figure H:** *Interplay between copying photo files and FS Creation, EXIF Creation, and FS Modified Dates.*

Here, the particular folder alleged to be the source of the contraband photos, is named “BKP.DellDimension8300-20090330,” and, according to its file listing came from the third, aberrant backup. The later part of the folder’s name, “20090330,” implies that it resulted from an automatic backup that occurred on March 30, 2009.<sup>97</sup> Further, the backup folder also had an FS Creation date of March 30, 2009.<sup>98</sup> These two data points strongly corroborate the government’s theory of the contraband photos being taken in 2005 and backed up to the backup hard drive in 2009.

Further, within the “Studies” subfolder of this backup, the EXIF Creation dates and the FS Modified dates for all photo files fall within a range from October 17, 2005, to December 30, 2005.<sup>104</sup> This implies that the photos were taken between those two dates. However, all the FS Creation dates for these same files are July 26, 2003.<sup>105</sup> Of course, this is impossible because one cannot

<sup>97</sup> *Id.*; *See also Id.* at Trial Tr. at 4792:20-21.

<sup>98</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 010, Finding 7.

<sup>102</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) GX 505A.

<sup>104</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Appendix B, Bates 015-217.

<sup>105</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Appendix B, Bates 015-217.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

back up a photo file two years before one has taken the photo. Moreover, the Canon camera in question was not manufactured until 2004.<sup>106</sup>

Since time travel is impossible, the most plausible explanation for these anomalies is tampering. The data here evidences that the tamperer(s), in an effort to be authentic, rolled their computer's clock back to 2003, perhaps thinking, 'Since I want the photos to look like they were taken in 2005, I'd better have my computer look like it was from 2003.' Then, the tamperer(s) manually copied the photo files from their computer to the backup hard drive, unbeknownst to them giving all the files FS Creation dates of July 26, 2003. Next, on the hard drive, the tamperer(s) manually changed the folder's name to "20090330," and its FS Creation date to March 30, 2009. However, the tamperer(s) either forgot to change, or were unaware of the need to change, the individual photo files' FS Creation dates from 2003 to 2009, thus leaving smoking gun evidence of tampering.

Moreover, the backup folder also has an FS Accessed date, or "Last Accessed" date, of July 28, 2003, evidencing that this was not a one-time fluke occurrence but rather the tamperer(s) kept their computer clock rolled back while they perpetrated the tampering over a period of days.<sup>107</sup>

---

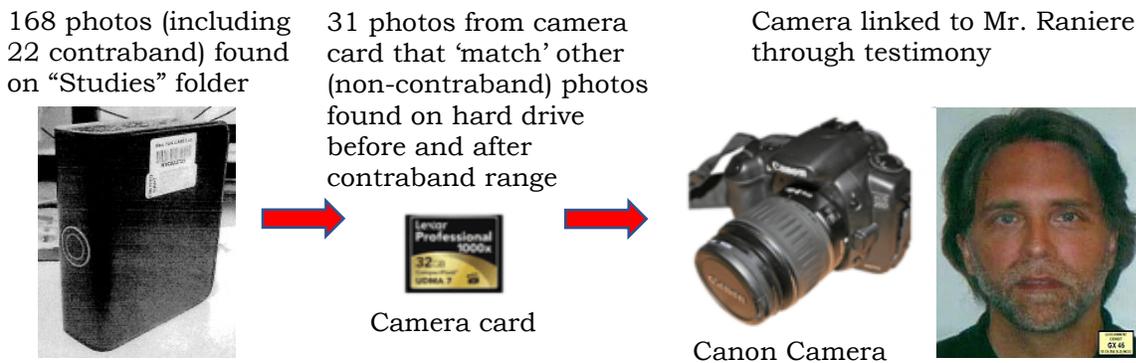
<sup>106</sup> DP Preview, Canon EOS 20D and preview (August 19, 2004) found at <https://www.dpreview.com/articles/1172584268/canon-eos20d>

<sup>107</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 010, Finding 7.

**The Government’s use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

**IV. Anomalies on Camera Card**

While the camera card was never alleged to contain any contraband images after it was seized by the FBI, the government used it in trial to link Mr. Raniere to the 22 alleged contraband photos found on the hard drive. The government’s evidence related that, since 31 of the non-contraband photo files from the camera card found in the Canon camera also appeared on the hard drive, *in the range before and after the contraband photos*, the contraband photos must also have come from the same camera, which had been linked to Mr. Raniere. The alleged link between the specific Canon camera and Mr. Raniere were two disparate descriptions from two witnesses who had seen Mr. Raniere with cameras in the past. These descriptions were, “Like a normal camera, like a camera with a flash. Not like a phone camera, like a – like a photographer’s camera,” and “There was a big camera. It was a big professional camera.”<sup>108</sup> Despite the Canon camera’s availability to the government, no witness was ever asked to identify it, nor shown the camera to confirm whether it was the item they were describing.



**Figure J:** Government’s trial narrative linking Raniere to contraband photos.

However, experts have found extensive evidence of tampering on the camera card and uncovered circumstances which strongly evidence that such tampering occurred *while the camera card was in FBI custody*.<sup>109</sup> Thus, the corroborative evidence from the camera card used by the government to link the Canon camera, and thus Mr. Raniere, to the alleged contraband photos resulted from tampering, therefore it was not competent evidence, and therefore the convictions that resulted therefrom should be vacated.

<sup>108</sup> Trial Tr. at 1536: 25 – 1537: 1; 2569; 2568: 24-25.

<sup>109</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt 1169-1 at Ex. D at Bates 006-007 Finding 3; Bates 012 Appendix A; Bates 032 conclusion; Bates 034 Finding 4; Bates 035-036 Finding 3 & 4; Bates 0054 Finding 6.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

**A. The Camera Card Was Altered on September 19, 2018, While in FBI Custody**

On September 19, 2018, FET Donnelly created a forensic copy of the hard drive.<sup>110</sup> However, also on September 19, 2018, before the camera card had been processed by the CART lab, the case agent for this case, SA Lever, checked the camera card out of Evidence Control for “review.” This is in direct violation of FBI policy which prohibits any examination of electronic evidence before it has been processed by the CART lab.<sup>111</sup> Thus, SA Lever checked out an evidence item that neither he, nor any other agent, was authorized to view or inspect at the time. **Kiper Ex. D, finding 3, Bates 35.**

Also, *on this same day*, September 19, 2018, the camera card was improperly accessed without a write-blocker and was irrevocably altered.<sup>112</sup> A write-blocker is a device that allows one to access digital evidence without writing to it, as writing to a piece of digital evidence destroys its integrity.<sup>113</sup>

Thus, because the camera card was accessed without a write-blocker, its FS Accessed dates (last accessed dates) were overwritten. Consequently, it is impossible to tell whether other alterations were made at that time or previously. Additionally, the FBI has never disclosed records of who accessed and altered the camera card on this date. **Ex D. findings 3 & 4, Bates 35.** The fact that an unknown *and unauthorized* person accessed the camera card *in an unauthorized manner* which destroyed the integrity of the item *on the same day* that Donnelly made a forensic copy of the hard drive in an *authorized* manner shows a level of coordination among FBI personnel regarding the hard drive and the camera card *both on and off the record*. This is damning since the alleged contraband photos had not been discovered yet, so the hard drive and camera card would not have been highly relevant to any criminality as alleged in the search warrant. **[CITE to SEARCH WARRANT.]**

**B. The Camera Card Was Most Likely Altered Between April 11, 2019, and June 11, 2019, While in FBI Custody**

On April 11, 2019, SFE Stephen and SFE Flatley conducted a forensic examination of the camera card.<sup>114</sup> SFE Flatley, using the forensic examining software “AccessData Forensic Toolkit,” version 6.3.1.26, found 42 photos on

---

<sup>110</sup> *Id.* at DX 961 at Bates 011; Bates 024

<sup>111</sup> *Id.* at DX 945; *See also* Dkt. 1169-1 at Ex. C at 21.

<sup>112</sup> *Id.* at Ex. D at Bates 006-007 Finding 3; Bates 012 Appendix A; Bates 032 conclusion; Bates 034 Finding 4; Bates 035-036 Finding 3 & 4; Bates 0054 Finding 6; *see also* Trial Tr. at 4966:24 - 4973:9.

<sup>113</sup> *Id.* at Trial Tr. at 4781:5-19.

<sup>114</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) at GX 521A – Forensic Report of Camera Card completed by SFE Flatley on April 11, 2019.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

the camera card.<sup>115</sup> However, his forensic examination found only four photos on the camera card (photo files 180-183) which 'matched' counterpart photos on the hard drive (photo files 180-183).<sup>116</sup> While four matching photos on a camera card from a camera linked to Mr. Raniere could have established a link between Mr. Raniere and the contraband photos on the hard drive, it was weak in terms of proving a direct connection beyond a reasonable doubt in front of a jury.

However, two months later, on June 11, 2019, SFE Booth conducted a *second* forensic examination of the camera card.<sup>117</sup> He used the same software, AccessData Forensic Toolkit, and the same version of the software, version 6.3.1.26, that Flatley had used in his April 11, 2019, forensic examination. However, SFE Booth's June 11, 2019, report incredibly found 37 new photos, of which 31 'matched' photos on the hard drive.<sup>118</sup>

**1. SFE Booth's Second Examination of the Camera Card on June 11, 2019, Was Conducted Under Highly Suspicious Circumstances**

A second forensic examination is very unusual and is strictly prohibited by FBI policy barring obtaining specific authorization from the executive management of the FBI Operational Technology Division.<sup>119</sup> Nonetheless, on June 7, 2019, during the last few days of trial, SA Lever, against FBI policy,<sup>120</sup> requested SFE Booth to complete a new examination of and report on the camera card.<sup>121</sup>

SA Lever requested this reexamination purportedly because SFE Flatley was going to be overseas and therefore unavailable to testify about his work on the April 11, 2019 camera card report.<sup>124</sup> However, according to the FBI's chain of custody log,<sup>125</sup> SFE Flatley turned over custody of the camera card to SA McGinnis on June 7, 2019, the same day SA Lever requested the second examination, thus SFE Flatley was not yet overseas. Moreover, since trial began on May 7, 2019, SFE Flatley *had been available to testify at any time during the previous four weeks of trial*. There was no legitimate need to reexamine the camera card and create a second report. The most plausible reason to do so is that new files and alterations had been made to the camera

---

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*; *See also Id.* at Dkt. 1169-1 at Ex. D at Bates 028-029 Appendix D, Figure 1 & 2.

<sup>117</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4903:1-7; DX 961 at Bates 029-030; see also GX 521A – Replacement Forensic Report of Camera Card completed by SFE Booth on June 11, 2019, hereafter "GX 521A Replacement."

<sup>118</sup> *Id.* at Dkt. 1169-1 Ex. D at Bates 028-32.

<sup>119</sup> *Id.* at Bates 037 Fn. 6.

<sup>120</sup> *Id.* at Ex. D at Bates 037 Fn. 6.

<sup>121</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 029.

<sup>124</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 029.

<sup>125</sup> *Id.* at DX 945.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

card and needed to appear on the camera card's forensic inventory prior to SFE Booth testifying.

The FBI's forensic lab, CART, has a policy for reexaminations that require approval from the executive management of the FBI Operational Technology Division.<sup>126</sup> However, SFE Booth did not obtain such approval. Instead, he only obtained approval from his acting supervisor, Supervising Special Agent, hereafter "SSA," Trenton Schmatz. SSA Schmatz did not have authorization to grant this approval, but he did so anyway.<sup>128</sup>

On June 10, 2019, the day before the reexamination, according to SFE Booth's testimony, SA Mills delivered the camera card to SFE Booth ***in an unsealed bag***.<sup>129</sup> This was more than fourteen months after the search team had collected it and on the fourth to last day of a trial that spanned 43 days. *There is no record of who unsealed this evidence nor at what point it was unsealed.* On June 11, 2019, the day before he took the stand at the tail end of trial, SFE Booth reexamined the camera card and completed a new report for the device.<sup>130</sup> SFE Booth's examination notes<sup>131</sup> end abruptly after he created the forensic copy of the camera card. Normally, details, such as the options a forensic examiner chose while processing the data with the forensic software as well as the final disposition of the original or derivative evidence would complete a normal CART forensic report. Strangely, these details were left out of SFE Booth's evidence notes.<sup>132</sup>

## **2. Photo Files 93, 94, 96, and 97 Are Bogus**

Four of the photographs that appeared for the first time on SFE Booth's June 11, 2019, report, photo files 93, 94, 96, and 97, appear on the surface to have matching counterpart photo files on the hard drive. This was used by the government at trial to support their theory that the alleged contraband photos on the hard drive were taken by the camera.<sup>133</sup> However, all three forensic experts hired by the defense after trial discovered a major blunder by the tamperer(s) regarding these four files; **despite photo files 93, 94, 96 and 97 having identical filenames and identical metadata on both the camera**

---

<sup>126</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 037 Fn. 6.

<sup>128</sup> *Id.* at Bates 037 Fn. 6. [SSA Trenton Schmatz is a supervisory special agent based on his title, he had insufficient authorization to grant the approval for reexamination of the camera card].

<sup>129</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4889:14-18.

<sup>130</sup> *Id.* at GX 521A Replacement; *See also Id.* at Trial Tr. at 4826: 6-17.

<sup>131</sup> *Id.* at DX 961 at Bates 030.

<sup>132</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 030.

<sup>133</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4857:2 -11 [linking the camera card with the camera]; 4858:2:20 [where the camera card report is described]; 4901:21 - 4902:3 [where SFE Booth describes what the camera card is and its relationship to the camera; and 4911:9-15 [where SFE Booth describes how many photos were on the camera card].

---

**card and hard drive, on the camera card, the thumbnails for these photos files are all of a blonde woman, whereas on the hard drive, the thumbnails for photo files 93, 94, 96, and 97 are all of a completely different woman - a brunette.**<sup>134</sup> On a normal backup, the camera card's photo files, to include their thumbnails, would have counterparts on the hard drive that are identical matches. Computers do not make such errors; thus, **this anomaly can only be due to manual tampering.**

Further, the thumbnails of photo files 93, 94, 96, and 97 from SFE Booth's June 11, 2019, camera card report are identical to the thumbnails of photo files 180, 181, 182, and 183 on this same camera card. Kiper, Ex. D, finding 1, Bates 4. Not only are they visually the same, but their MD5 Hash, or digital "fingerprints," are identical. Kiper, Ex. D, Bates 23, Appendix C, Table 1. Of note, photo files 180, 181, 182, and 183 were the *only* four files in common between the hard drive and the camera card according to the original April 11, 2019, camera card report and the original April 11, 2019, hard drive report. Kiper, Appendix C, Bates 22. The fact that photo files 93, 94, 96, and 97 are exact copies of photo files 180, 181, 182, and 183, informs us how the tamperer(s) likely created the bogus photo files 93, 94, 96, and 97 - as well as all 37 new photo files from the June 11, 2019, report. Because the hard drive had already been checked into evidence, forensically copied, examined in CART, and loaded into the Case Agent Investigative Review system, hereafter the "CAIR system," the tamperer(s) would not have had direct access to the hard drive and thus could not copy files directly from the hard drive to paste into the camera card. Thus, the safest way to reverse-engineer 'matches' between the hard drive and the camera card would be to replicate the four proven matches - photo files 180-183. Thus, on a computer, the tamperer(s) copied the four photo files 180, 181, 182, and 183, and pasted them. They then renamed the pasted copies to 93, 94, 96, and 97, respectively. They then altered the metadata of the copies to match the metadata of photo files 93, 94, 96, and 97 as found on the April 11, 2019, hard drive report, to make the photo files on both devices appear to match. Kiper, Ex. D, Finding 1, Bates 4.

Such anomalies can only reasonably be explained by manual tampering. Since the camera card was in the custody of the FBI during the time of the appearance of these anomalies, members of the FBI are the only reasonable suspects.

### **3. Thirty-Seven New Files Appear to Have Been Added to the Camera Card Between April 11, 2019, and June 11, 2019, While It Was in FBI Custody**

SFE Booth used the identical software and identical version of the software for his June 11, 2019, camera card report that SFE Flatley used for his April, 11,

---

<sup>134</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 003, Finding 1.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

2019, camera card report. However, SFE Booth's report had an additional 37 new photos than did Flatley's.<sup>135</sup> Accordingly, with these new 37 photos, the government now had a total of 31 photos from the camera card that 'matched' photos on the hard drive, significantly more than the four matches that SFE Flatley had originally found. **Kiper, finding 2, bullet point 2, Bates 5 AND (together with) Kiper, Appendix B, Bates 15-21.**

Damningly, while the 42 photo files originally found by SFE Flatley were all viewable, **none** of the new 37 photo files from SFE Booth's June 11, 2019, forensic examination were viewable.<sup>136</sup> More damning, none of the MD5 hashes (digital fingerprints) for the new files on the camera card report match their namesakes on the hard drive report. Mismatched MD5 hashes means they are not the same files. **Kiper, Bates 5.** Again here we see that, **despite having identical filenames and identical metadata on both the camera card and hard drive, which are easily to change, the new 31 matching photo files in Booth's camera card report do not truly match their counterpart photo files on the hard drive report.** **Kiper, Bates 6.**

The pattern of tampering and attempted cover up is obvious here. Due to the coordination required between the hard drive, which was in the FBI's custody, and the camera card, which was in the FBI's custody, the FBI must have been complicit.

**4. The Arrangement of the Thirty-Seven New Files on the Camera Card Indicates That They Were Placed There Manually Rather Than as a Result of Someone Taking Photos**

Before SFE Booth's June 11, 2019, camera card report, there were only four photo files in common between the camera card and backup hard drive (180-183). **Kiper, Ex. D. Bates 28.** Eight of the newly appearing photo files (172-179) are located immediately before these common photo files. Next is a range of alleged contraband photos (184-191). Then, eight more of the newly appearing files (193-200) follow right after the alleged contraband range. The 'neat symmetry' of sixteen of the newly appearing photo files appearing before and after the alleged contraband photos fit the government's narrative precisely. Such newly appearing 'neat symmetry' in *precisely* the locations the government would need for its narrative is mathematically improbable and thus is more likely the result of tampering rather than coincidence.

---

<sup>135</sup> *Id.* at Dkt. 1169-1 at Ex. D at Bates 028-32.

<sup>136</sup> *Id.* at Bates 005, Finding 2; Bates 028-29, Appendix D; Ex. E at Bates 003-02, Finding 1; Ex. F at Bates 004-005.

**The Government’s use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

<b>Photo File #</b>	
<b>172</b>	8 newly appearing photo files
<b>173</b>	
<b>174</b>	
<b>175</b>	
<b>176</b>	
<b>177</b>	
<b>178</b>	
<b>179</b>	
180	The only photos files initially in common between the camera card and the backup hard drive
181	
182	
183	
184	2 <sup>nd</sup> range of alleged contraband
185	
186	
187	
188	
189	
190	
191	
<b>193</b>	8 more newly appearing photo files
<b>194</b>	
<b>195</b>	
<b>196</b>	
<b>197</b>	
<b>198</b>	
<b>199</b>	
<b>200</b>	

**Figure K:** Showing the ‘neat symmetry’ of sixteen of the photo files which newly appeared on Booth’s June 11, 2019 Camera Card Report.

There is yet another example of this ‘neat symmetry’ on Booth’s June 11, 2019, Camera Card Report which evidences intentional placement rather than random photo taking behavior. Notably, on the hard drive, under the “Studies” folder, there are three ranges of photos each with its own subfolder<sup>139</sup>:

- Photo files 79-89 of “MsK” (Kathy)
- Photo files 90-98 of “Df” (Daniela)
- Photo files 99-108 of “Mnp” (Marianna and Pam)

<sup>139</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) at GX 505.

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

Yet suspiciously, only photo files 81 to 100 are among the files to newly appear on Booth's June 11, 2019 camera card report. (Figure L, below.) Photo files 79 and 80 from the Kathy range and photo files 101 to 108 from the Marianna and Pam range are missing.

It is extremely unlikely that a normal camera user would have taken photos, saved them all to a hard drive and then go back to the camera and delete segments of photo ranges in this manner. For instance, a normal camera user would not take eleven photos of Kathy, photo files 79-89, back up all eleven to a hard drive, and then go back to the camera to delete only photos 79 and 80. Likewise with the range of Marianna and Pam, a normal camera user would not take exactly ten photos, photo files 99-108, back up all ten, and then go back to the camera and delete only the last eight photos, 101-108. In contrast, with the range of Daniela, no photo is deleted. This behavior is inexplicable and would not be reasonable camera user behavior.

However, it is reasonable that someone who wanted a stronger relationship between the camera card and the hard drive picked a nice, round number of twenty files, photo files 81-100, and manufactured them so that they may appear on Booth's June 11, 2019, camera card report to line up with significant ranges of photos files present on the April 11, 2018, hard drive report.<sup>143</sup>

---

<sup>143</sup> *Id.* at Bates 35, Finding 3.

**The Government’s use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

<b>Subject</b>	<b>April 11, 2019 Hard Drive</b>	<b>April 11, 2019 Camera Card</b>	<b>June 11, 2019 Camera Card</b>
Kathy	79		
	80		
	81		<b>81</b>
	82		<b>82</b>
	83		<b>83</b>
	84		<b>84</b>
	85		<b>85</b>
	86		<b>86</b>
	87		<b>87</b>
	88		<b>88</b>
	89		<b>89</b>
Daniela	90		<b>90</b>
	91		<b>91</b>
	92		<b>92</b>
	93		<b>93</b>
	94		<b>94</b>
	95		<b>95</b>
	96		<b>96</b>
	97		<b>97</b>
	98		<b>98</b>
Marianna & Pam	99		<b>99</b>
	100		<b>100</b>
	101		
	102		
	103		
	104		
	105		
	106		
	107		
	108		

**Figure L:** Showing the ‘neat symmetry’ of exactly twenty photo files newly appearing on Booth’s June 11, 2019, Camera Card Report.

**The Government’s use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

The camera card file listing from SFE Booth’s June 11, 2019, report shows a sequence of recovered photos and remnants of photos, allegedly the source of the photos on the hard drive. However, there are large gaps of missing photo files on the camera card, compared to the complete sequence on the hard drive.<sup>146</sup>

<b>April 11, 2019 Hard Drive Report</b>	<b>June 11, 2019 Camera Card Report</b>
MISSING	21-41
MISSING	42
43-80	<b>MISSING</b>
81-100	81-100
101-149	<b>MISSING</b>
<b>150-163 [alleged contraband]</b>	
164-165, 168-169	
172-179 sans 173	172-179
180-183	180-183
<b>184-191 [alleged contraband]</b>	<b>MISSING</b>
194, 197-199	193-200
	<b>MISSING</b>
203-223	
MISSING	224-243, sans 226, 232, and 240

**Figure: K** Comparison of June 11, 2019, Camera Card report and April 11, 2019, Hard Drive report.<sup>147</sup>

Note that where the above chart states, “MISSING,” in the June 11, 2019, Camera Card Report, **there was no data, not even remnants of deleted data, able to be recovered.** This means that either the photo files were never there to begin with, they were forensically deleted “wiped,” or they were deleted by the user and overwritten by the camera taking subsequent photos. Of these options, a camera user forensically wiping the camera card only in these particular swaths is not consistent with normal use of a camera, where the user might review and choose to occasionally delete unwanted photographs as desired. Moreover, it would not make logical sense for a camera user to take out the camera card from the camera, use a computer to forensically wipe some of the files, which requires specialized software, and then leave everything

<sup>146</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 028-029, Appendix D.

<sup>147</sup> Illustration of Appendix D found at *Id.*

**The Government's use of altered evidence and false testimony by the FBI in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.**

---

else. Further, the camera card here was not close to being full; thus, any subsequent photos could not have completely written over remnants of deleted photo files. [CITE.]

While there is an argument that Mr. Raniere could have wiped swaths of photo files from the camera card to remove the contraband photos, the deleted swaths also include other photos that were not contraband. Additionally, this theory of Mr. Raniere forensically deleting random swaths of data from the camera card to cover up his crime loses ground if one considers the government narrative at trial that Mr. Raniere created contraband photos in 2005 on a camera, then, in 2009, backed them up to a hard drive that multiple other people had access to, and simply just left them there from 2009 to 2018 - a period of nine years - for the FBI to later find.

There is no need to contort logic to find an explanation for these missing swaths of data; the pattern here is entirely consistent with a tamperer looking at photo files on the hard drive and manufacturing 'matches' on the camera card. Because the tamperer(s) were merely adding manufactured 'shells' of photo files in certain swaths to the camera card to link the camera card to the hard drive, there would be nothing, not even remnants of deleted photos files, in the "Missing" sequences. Here, because the 37 new files were not viewable and had incomplete data, given the evidence we have now, these files are likely 'shell' files thus strongly supporting the tampering theory.

The alleged contraband photos, photo files 150-163 and 184-191, appear in neither the April nor the June forensic reports the government produced of the camera card. However, if the government's narrative of the contraband photos originating on the Canon camera and then being backed up to the hard drive was true, then **at least some** remnants of these photos would be found on the camera card.<sup>150</sup> However, no such remnants were found. Thus, the government's narrative must be false.

---

<sup>150</sup> Raniere, supra, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 029, Observations.

**V. Perjury by Brian SFE Booth, FBI Senior Forensic Examiner**

During his testimony on the third-to-last and second-to-last day of evidence during jury trial, SFE Booth testified falsely while under oath on the stand. Further, in all three areas where SFE Booth committed perjury, he specifically covered up the tampering and thus enabled the government's false narrative.

**A. SFE Booth Committed Perjury in Testifying that EXIF Data Was Difficult to Change**

SFE Booth testified while under oath that metadata, such as EXIF data and "creation dates," was difficult to change and, in fact, was designed to be difficult to change.<sup>151</sup> This testimony regarding the reliability of the 2005 dates helped the government's narrative that the 22 photos of Camila were contraband.<sup>152</sup> However, in actuality, EXIF data is quite easy to change, and anyone can do so on a home computer with no special software needed. Moreover, simply performing an internet search for "change EXIF data on photo" yields a multitude of free tools appearing in the search results that can all easily change EXIF data.<sup>153</sup> In fact, changing Metadata such as EXIF data and creation dates, is as easy as changing words or sentences in a Microsoft Word document. SFE Booth, *as a senior forensic examiner for the FBI*, had to have known this, but chose to lie about it on the stand.

Additionally, as of late August 2022, new evidence has surfaced that also corroborates that the government used false testimony in this case. In 2016, *three years before this trial*, SFE Flatley, who was a material witness in this case before being abruptly reassigned to Ghana, Africa at the last moment, testified as a qualified expert in *United States v. Hirst* 15-cr-643 (PKC) (S.D.N.Y. Apr. 18, 2022) **that the FBI does not rely on metadata alone in determining a document's date because metadata can be "manipulated."**<sup>154</sup> Flatley's testimony in *Hirst* is the exact opposite of the testimony that the government solicited from SFE Booth in this case. It is no wonder that SFE Flatley was assigned to Ghana a mere two days before he was set to testify. It is no wonder that *someone* in the government, or a group, wanted to, *and needed to*, substitute SFE Booth's testimony for SFE's Flatley's testimony. As the government itself said, **"the child pornography is also at the heart of our racketeering conspiracy."** Without the racketeering charges, the government would have faced substantial venue, jurisdiction, and statute of limitations issues.

---

<sup>151</sup> *Id.* at Trial Tr. at 4818:24-4820:20, 4830:3-11, 4977:11-14.

<sup>152</sup> *Id.* at Trial Tr. at 5371:16-24; 5571:13-5572:3

<sup>153</sup> *Id.* at Ex. D at Bates 042-046, Modifying Photograph EXIF Data.

<sup>154</sup> *United States v. Hirst*, 15-cr-643 (PKC) Dkt. 316 – Trial Transcript (September 20, 2016) hereafter "Galanis Trial Tr.," at 939:15-18; 941:6-12 [emphasis added]; see also Exhibit B attached herein.

**B. SFE Booth Committed Perjury in Testifying that It Was Not Unusual to Receive Evidence that is Unsealed with No Record of the Unsealing**

SFE Booth also testified that it was not unusual in the FBI to receive opened or unsealed evidence items where there was no record of who unsealed the evidence.<sup>155</sup> However, in actuality, all physical evidence admitted into court must have a chain of custody proving that it was unaltered. As part of this process, evidence must be sealed.<sup>156</sup> This is a basic rule of evidence. In fact, most people who watch courtroom dramas on television know that evidence must be sealed and have a clear chain-of-custody.

SFE Booth's camera card report is materially different from Flatley's prior camera card report such that 37 new, *and defective*, files appeared on Booth's report which coincidentally bolstered the prosecution's case regarding the alleged contraband photos. Thus, it would have been imperative to have sealed evidence with a documented, clear chain-of-custody to prove that no wrongdoing happened to the camera card. Of course, we do not have that here and, not coincidentally, we have a small mountain of evidence that the camera card was tampered with.

**C. SFE Booth Committed Perjury in Testifying that There Was No Need to Create a Chain-of-Custody Log Every Time an Evidence Item Is Opened**

Relatedly, SFE Booth testified that there was no need to create a chain-of-custody log every time an evidence item is opened.<sup>157</sup> However, in actuality, all physical evidence to be admitted into court must have a chain of custody proving that it was unaltered. Therefore, anytime a bag of sealed evidence is opened, there needs to be a log recording the opening of the evidence item.<sup>158</sup> Thus, his testimony was not truthful. *As a senior forensic examiner for the FBI*, SFE Booth must have known this basic rule of evidence as he is well aware of how evidence is logged and categorized as it makes its way through collection and analysis.

---

<sup>155</sup> *Raniere, supra*, 18-CR-204 (NGG) Trial Tr. at 4886:15-4887:23.

<sup>156</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 033-035, Finding 1

<sup>157</sup> *Id.* at Trial Tr. at 4887:21-4888:4.

<sup>158</sup> *Id.* at 18-CR-204 (NGG) Dkt. 1169-1 at Ex. D at Bates 035, Finding 5.

## **VI. Prosecutorial Anomalies**

As early as September 13, 2018, one of the lead prosecutors in this case, AUSA Penza had been referencing additional charges, specifically tied to discussion of discovery around the 60 devices found at the two residences during execution of the search warrant on March 27, 2018.<sup>159</sup> On January 9, 2019, AUSA Penza, told the Court, “[T]he government continues to expect a superseding indictment in this case... [T]here are a number of factors that are weighing into the timing considerations for a superseding indictment.”<sup>160</sup> However, as previously noted, the FBI did not allegedly discover the contraband photos until February 21, 2019.<sup>162</sup> This would not happen until 44 days after her January 9, 2019 statement to the court and a whopping 162 days after her September 13, 2018 statement to the court.

On March 13, 2019, when the government did file its second superseding indictment, the only new additions were the allegations regarding possession of child pornography and sexual exploitation of a minor. Since the only difference between the first superseding indictment and the second superseding indictment was new charges based on the alleged contraband photos, this raises the standard question of, ‘What did Ms. Penza know and when did she know it?’

AUSA Penza’s impossibly precognitive statements to the court months before the alleged contraband photos were found, should be considered disturbing, especially in light of the irrefutable and expert-validated proof of government tampering presented in this document.

---

<sup>159</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Scheduling Conference Transcript (September 13, 2018), at 13: 24 -14: 8.

<sup>160</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Motion Hearing Transcript (January 9, 2019) hereafter “Mot Tr., (1/9/18)” at 4:4-25.

<sup>162</sup> *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 594-2 – Second Lever Aff at ¶ 8 & 11 (filed under seal); *See also* Dkt 618 at 2.

## **CONCLUSION**

Fundamental fairness and every Accused's right to a fair and just trial is the cornerstone of our criminal justice system. As this document establishes, Mr. Raniere was denied these fundamental rights in the jury trial of *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282 when the government presented false and manipulated evidence. The Court must move on this immediately and grant a stay of the appeal so that this injustice may be addressed and remedied at the earliest possible time. It is not a statutory time limit that should motivate the Court to address this post-haste, but rather the need to prevent further injustice.

Not only is there a manifest injustice each second that Mr. Raniere continues to spend behind bars based on false and manipulated evidence, but the bad actors within government who perpetrated this planting, manufacturing, and tampering of evidence, continue to work on and be involved with new cases. Whether they are engaging in this same criminal conduct on other cases or not, when the tampering in this case is finally acknowledged in Court and Mr. Raniere is vindicated of these heinous charges, **the actions of any governmental actors subsequently proven to be involved, will need to be questioned and re-examined in all other cases in which they were allowed to work.** Delaying the District Court's review and response to the governmental tampering here, which the evidence shows to a scientific certainty, will only allow this harm to continue **and will negatively impact many other Accused individuals, as well as many other cases which, in turn, will negatively impact the functioning of the court system.**