

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

Thurgood Marshall U.S. Courthouse 40 Foley Square, New York, NY 10007 Telephone: 212-857-8500

MOTION INFORMATION STATEMENT

Docket Number(s): 20-3520

Caption [use short title]

Motion for: TO HOLD APPEAL IN ABEYANCE PENDING RULE 33 MOTION.

Set forth below precise, complete statement of relief sought:

See attachments.

United States of America v. Ranieri

MOVING PARTY: Keith Ranieri

OPPOSING PARTY: United States of America

- Plaintiff Defendant
Appellant/Petitioner Appellee/Respondent

MOVING ATTORNEY: Joseph M. Tully, Esq.

OPPOSING ATTORNEY: Tanya Hajjar, Esq.

[name of attorney, with firm, address, phone number and e-mail]

TULLY & WEISS ATTORNEYS AT LAW

UNITED STATES ATTORNEY'S OFFICE - EDNY

713 Main Street, Martinez, CA 94553

271 Cadman Plaza East Brooklyn, NY 11201

Joseph@Tully-Weiss.com (925) 229-9700

Tanya.Hajjar@usdoj.gov (718) 254-6351

Court- Judge/ Agency appealed from: Hon. Nicholas G. Garaufis, Eastern District of New York

Please check appropriate boxes:

FOR EMERGENCY MOTIONS, MOTIONS FOR STAYS AND INJUNCTIONS PENDING APPEAL:

Has movant notified opposing counsel (required by Local Rule 27.1): Yes No (explain):

Has this request for relief been made below? Yes No

Has this relief been previously sought in this court? Yes No

Requested return date and explanation of emergency:

Opposing counsel's position on motion: Unopposed Opposed Don't Know

Does opposing counsel intend to file a response: Yes No Don't Know

Is oral argument on motion requested? Yes No (requests for oral argument will not necessarily be granted)

Has argument date of appeal been set? Yes No If yes, enter date: Argument given on May 3, 2022

Signature of Moving Attorney:

/s/ Joseph M. Tully Date: 10/6/2022 Service by: CM/ECF Other [Attach proof of service]

ORAL ARGUMENT REQUESTED

Case No. 20-3520

**UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT**

UNITED STATES OF AMERICA
Appellee,

v.

KEITH RANIERE,
Defendant/Appellant,

**DEFENDANT-APPELLANT MOTION TO HOLD CASE IN ABEYANCE
PENDING RULE 33 MOTION**

Pursuant to Rule 27 of the Federal Rule of Appellate Procedure, Defendant-Appellant, Keith Raniere, by and through his counsel, hereby respectfully moves the Court to hold the above-captioned appeal in abeyance pending disposition of Mr. Raniere's post-judgment Rule 33 motion in the district court.

BACKGROUND

The instant appeal concerns the entry of judgment for *United States v. Raniere* 18-cr-204-1 (NGG) (VMS), entered on October 30, 2020. Dkt. 969.

On November 11, 2020, Mr. Raniere filed a notice of appeal. Dkt. 11-1.

On May 7, 2021, Mr. Raniere filed his appellate brief in this matter, with a supplemental appellate brief filed on November 5, 2021. Dkt. 102; 153.

On April 28, 2022, Mr. Raniere filed a motion to hold the instant appeal in abeyance pending filing a motion under Rule 33 of the Federal Rules of Criminal Procedure based on newly discovered evidence. Dkt 202.

On April 29, 2022, this Court denied Mr. Raniere's motion to hold the instant appeal in abeyance pending disposition of an anticipated Rule 33 motion. Dkt. 215.¹

However, on May 3, 2022, Mr. Raniere filed a motion, in the United States District Court for the Eastern District of New York, under Rule 33 of the Federal Rules of Criminal Procedure based on the newly discovered evidence that indicated that the government used false testimony and tampered evidence in obtaining a conviction against Mr. Raniere at trial. *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1168-1169.

¹ Counsel is aware of Local Rule of 27.1(g);(h) and submits to the Court that the instant motion is not a motion for reconsideration but is rather a de novo motion to hold this case in abeyance in that Appellant has now filed a Rule 33 motion in the lower district court, as well as a supplement in the same court. *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1168-68; 1176-1176-1. Further, Appellant's legal team was recently made aware, through privileged correspondence, of a material government witness' prior testimony in *United States v. Hirst*, 15-cr-643 (PKC) (SDNY Apr. 18, 2022), which bolsters the issues raised by Appellant in his Rule 33 pleadings and will likely be dispositive to the issues raised therein.

Later that day, May 3, 2022, Mr. Ranieri presented oral argument in the instant appeal by and through counsel in this Court. Dkt. Entry. 218. There was no overlap in the issues presented in oral arguments and the tampering findings submitted to the District Court in the Rule 33 motion.

On May 9, 2022, the District Court deferred consideration of the Rule 33, pursuant to Rule 33(b)(1) and 37(a)(1) of the Federal Rules of Criminal Procedure, indicating that the matter was sub judice as a result of the oral argument in this appeal. *United States v. Ranieri*, 18-cr-204-1 (NGG) (VMS) Order entry May 9, 2022.

On June 17, 2022, Mr. Ranieri filed a supplemental motion in the United States District Court for the Eastern District of New York, pursuant to Rule 33 of the Federal Rules of Criminal Procedure based on the newly discovered evidence that the government violated Mr. Ranieri's constitutional due process rights by withholding material exculpatory evidence in violation of *Brady v. Maryland*, 373 US 83 (1963) and its progeny; violated *California v. Trombetta*, 467 US 479 (1984), by failing to retain potentially exculpatory evidence in bad faith and by destroying said evidence via the undisclosed violations by the FBI of "critical evidentiary protocol;" and interfered with Mr. Ranieri's right to effective assistance of counsel by preventing his trial counsel from performing independent investigation via the government's withholding of *Brady* material and destruction

of evidence in violation of *Trombetta. Ranieri, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1168-69.

Mr. Ranieri now moves this Court, by and through his counsel, to hold this appeal in abeyance to allow for the resolution of the two pending Rule 33 matters as there exists clear,² substantive constitutional injuries uncovered by new evidence that may render appellate review unnecessary or at the very least will clarify the issues for this Court to resolve.

DISCUSSION

This Court should hold the appeal in abeyance pending the resolution of Mr. Ranieri's pending Rule 33 motion, as well as its supplement, both filed in the lower court, as resolution of the pending motions will likely affect the course of the current appeal. "[T]he power to stay proceedings is incidental to the power inherent in every court to control the disposition of the causes on its docket with economy of time and effort for itself, for counsel, and for litigants." *Landis v. N. Am. Co.*, 299 US 248, 255 (1936). Where a post-judgment motion creates the "possibility that the order complained of will be modified in a way which renders

² **Exhibit A.**, in support of this motion is a plain language restatement of the complex and technical newly discovered evidence finding manually altered digital evidence in *United States v. Ranieri*, 18-cr-204-1 (NGG) (VMS). **Exhibit B.**, is an analysis of conflicting FBI testimony regarding EXIF Data, completed by Dr. J. Richard Kiper, PhD, former FBI special Agent. *See also Ranieri, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D; Ex. D1.

judicial review unnecessary,” *Stone v. INS*, 514 US 386, 392 (1995), holding the appeal in abeyance will serve the interests of this Court’s judicial economy, economy of time and effort for counsel and the parties in this case, and more importantly, the overall ends of justice.

Although Mr. Ranieri believes that the instant appeal does raise significant and weighty issues deserving the Court’s attention, if the appeal is not held in abeyance, the case may proceed on an inefficient track resulting in the waste of judicial resources. However, above all, if the appeal is not held in abeyance, the manifest injustice of blatant evidence tampering, which has now been irrefutably demonstrated in Exhibit A, and which was used by the government to obtain a conviction in the District Court will continue to be ignored; such is not justice.

The issues raised now in Mr. Ranieri’s Rule 33 motion, as well as its supplement, include the use of false testimony by the government to obtain a tainted conviction of Mr. Ranieri;³ the use of altered evidence by government

³ **Exhibit B.** – Analysis of Conflicting FBI Testimony Regarding EXIF Data, by J. Richard Kiper, PhD, PMP: Newly discovered evidence indicates that government prosecutors suppressed impeaching prior testimony of a key government witness in violation of *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. United States*, 405 U.S. 150 (1972). The same evidence buttresses the contention that prosecutors likely solicited false testimony and allowed the same to go uncorrected to obtain a tainted conviction of Mr. Ranieri in violation of due process. *See Giglio, supra*, at 153; *Napue v. Illinois*, 360 US 264, 269 (1959). [“Due process requires not only that the prosecutor avoid soliciting false testimony but that he not sit idly by and allow it to go uncorrected when it is given.”].

prosecutors to obtain a tainted conviction of Mr. Ranieri;⁴ and the government's interference with Mr. Ranieri's right to effective assistance of counsel at trial. If the district court finds that these issues were violative of Mr. Ranieri's constitutionally mandated due process rights, and acts accordingly in the interest of justice, the instant appeal would be rendered moot by a consequent new trial in the district court. Moreover, the newly discovered information that the government, *in the eleventh hour of trial*, swapped out one material FBI witness, whose testimony would have **exculpated** Mr. Ranieri, with another material FBI witness, whose perjurious testimony **wrongly inculpated** Mr. Ranieri,⁵ further corroborates the findings regarding tampering and creates more urgency for addressing them in the District Court.

Accordingly, holding the appeal in abeyance is appropriate here because it will promote "economy of time and effort" for the Court, counsel, and parties. *See Landis*, 299 US at 255. Once the District Court resolves the pending motions below, the issues for this Court to resolve will be clarified and the appeal can proceed, if it has not been rendered moot.

⁴ **Exhibit A.** – Simplified summary of the expert opinion of Dr. James Richard Kiper, Ph. D regarding discovery of altered digital evidence in *United States v. Ranieri*; a comprehensive report in regard is attached in support of Mr. Ranieri's Rule 33 matters found at *United States v. Ranieri*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.

⁵ **Exhibit B**, *supra*.

For the foregoing reasons, the Court should hold in abeyance this case pending the district court's resolution of Mr. Ranieri's post-judgment Rule 33 motion and supplement.

Dated: October 5, 2022.

Respectfully submitted,

/s/ Joseph M. Tully
Joseph M. Tully
(CA Bar. No. 201187)

**DECLARATION OF JOSEPH M. TULLY IN SUPPORT OF MOTION TO
HOLD APPEAL IN ABEYANCE PENDING RULE 33 MOTION**

I, JOSEPH M. TULLY, am an attorney in good standing admitted to practice in this Court, and affirm under penalty of perjury pursuant to 28 USC § 1746 as follows:

1. I represent the Defendant/Appellant in the above-captioned matter.
2. I submit this affirmation in support of Appellant's motion to hold his appeal in abeyance pending the determination of a Rule 33 motion and supplement thereto, which the Appellant has now filed in the District Court in *United States v. Raniere*, 18-CR-204 (NGG) (VMS) Dkt. 1169 and 1176.
3. During the pendency of this action, I reviewed the forensic expert reports of Dr. James Richard Kiper, Ph.D., Steven Abrams, and Wayne B. Norris, filed in support of Appellant Rule 33 motion. *Raniere, supra*, 18-CR-204 (NGG) (VMS)Dkt 1169-1 at Ex. D; E; & F. I used these reports as well as the attached Exhibit B. – Analysis of Conflicting FBI Testimony Regarding EXIF Data, by J. Richard Kiper, PhD, PMP, in drafting Exhibit A. – Plain language explanation of the expert opinion of Dr. James Richard Kiper, Ph. D regarding discovery of altered digital evidence in *United States v. Raniere*. Exhibit A is able to present the tampering in *flagrante delicto* as opposed to the vastly more technical expert reports attached to the Rule 33 motion which, by their nature of having to be

technical, necessarily obfuscate the everyday human conduct in manufacturing the tampered evidence presented by the government at trial against Mr. Ranieri.

However, Exhibit A is meticulously cited and, despite being written in plain language instead of the technical language of the expert findings, is still accurate and consistent with them.

4. Further, I was recently made aware, through privileged work product investigation, of testimony from 2016 in a different case provided by a material witness in this case, one of the forensic examiners who made findings to a key piece of evidence. His previous testimony from 2016 in the different case, *despite being directly on point with the main issue for the main charges in this case, directly contradicts the government's narrative used at trial in 2019 against Mr. Ranieri.* Had the government not swapped out this witness and had he testified consistently with his 2016 testimony on this exact issue, which is also consistent with lay experience as well as defense expert findings, it would have undermined the most important evidence at the heart of the government's case. Damningly, this examiner was reassigned to Ghana, Africa just days before he would have testified. While I knew about the reassignment previously, recently becoming aware of his previous testimony from 2016, which directly contradicting the government's narrative used at trial, puts a new light on the most probable reason behind his reassignment – nefarious intent by government actors.

5. Attached hereto as Exhibit A is a plain language explanation of the findings reached by the forensic experts noted herein regarding the government's use of manually altered evidence and false testimony in *United States v. Ranieri* 18-CR-204 (NGG) (VMS).

6. On behalf of Appellant, I respectfully submit Exhibit A attached hereto and all other supportive material attached hereto in support of Appellant's motion to hold the instant appeal in abeyance.

Dated: October 5, 2022.

Respectfully submitted,

/s/ Joseph M. Tully

Joseph M. Tully

(CA Bar. No. 201187)

Exhibit A

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. Raniere (E.D.N.Y. 2019) 384 F. Supp. 3d 282**



FIAT JUSTITIA RUAT COELUM

“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. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.

[Filed October 6, 2022.]

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.

TABLE OF CONTENTS

I.	INTRODUCTION	4
II.	ANOMALIES WITH SEARCH & EVIDENCE HANDLING.....	6
III.	ANOMALIES WITH EVIDENCE COLLECTION, PROCESSING, & ANALYSIS	10
IV.	ANOMALIES ON THE HARD DRIVE	14
	A. The Backup Itself.....	14
	B. Folders and Subfolders	15
	C. Files Within the “Studies” Folder.....	17
	1. Metadata Regarding Daylight Savings Time Was Manually Altered to Appear as If It Was Automatically Done by a Computer.....	19
	2. Metadata On at Least One Photo Was Falsified to Cover Up That the Photo Had Been Altered	21
	3. File System Creation Dates Impossibly Precede Both the Date the Photos Were Allegedly Taken and the Date the Photos Were Allegedly Backed Up.....	24
V.	ANOMALIES ON THE CAMERA CARD.....	27
	A. The Camera Card Was Altered on September 19, 2018, While in FBI Custody.....	28
	B. The Camera Card Was Most Likely Altered Between April 11, 2019, and June 11, 2019, While in FBI Custody.....	28
	1. Senior Forensic Examiner Booth’s Second Examination of the Camera Card on June 11, 2019, Was Conducted Under Highly Suspicious Circumstances.....	29
	2. Photo Files 93, 94, 96, and 97 Are Bogus.....	30
	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.....	32
	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	32
VI.	PERJURY BY FBI SENIOR FORENSIC EXAMINER BRIAN BOOTH	36
	A. Senior Forensic Examiner Booth Committed Perjury in Testifying that EXIF Data Was Difficult to Change	36
	B. Senior Forensic Examiner Booth Committed Perjury in Testifying that It Was Not Unusual to Receive Evidence that is Unsealed with No Record of the Unsealing	37

**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.**

C. Senior Forensic Examiner 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
VIII. CONCLUSION.....	39

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.

I. INTRODUCTION

During the jury trial in *United States v. Raniere* (E.D.N.Y. 2019) 384 F. Supp. 3d 282,¹ 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 drive² of a female, identified at trial as “Camila.”³ 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: (1) that the 22 photos were taken when Camila was under 18, and (2) that the photos were taken by Keith Raniere.

To show Camila was under the age of eighteen in the photos, the government used 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.⁴ Other metadata involved were File System dates, such as “Creation,” “Modified,” and “Accessed.” In trial, the government argued that **because EXIF data cannot be easily modified**, and because the metadata and EXIF data for the 22 photos indicated that they were taken in 2005 when Camila would have been 15 years old, Camila was therefore underage in the photos.

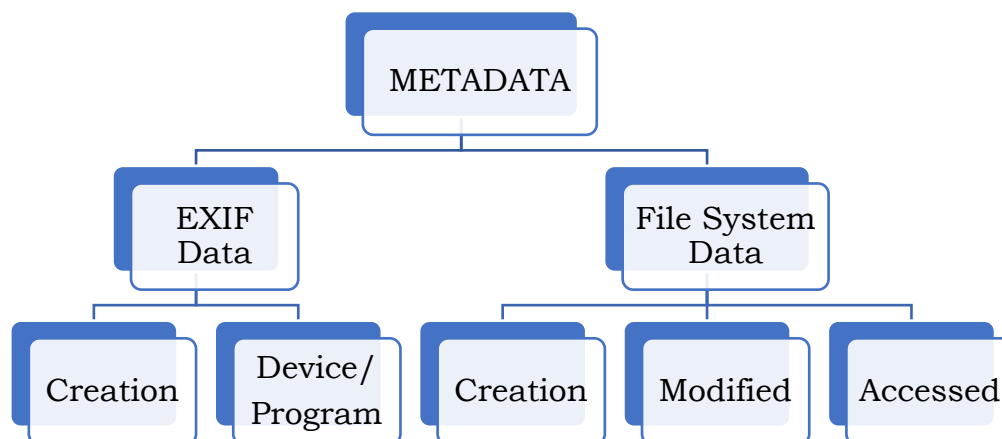


Figure A. Hierarchy of Metadata types.

¹ 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).

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

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

⁴ *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.

I. Introduction

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 which purportedly held the backup data of three different computers.⁵ 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 card⁶; (3) Mr. Raniere then downloaded the 22 photos off the camera card onto a Dell computer; and (4) that the Dell computer was then backed up to the hard drive.

However, after trial, three top digital forensic experts⁷ 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 and only partial 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. 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 backup 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."***⁸

Such demonstrable and *provable* criminality in manufacturing, fabricating, and tampering with evidence by bad government actors, cannot be allowed to stand. The longer such manifest injustice is ignored, the greater the ripple effects will be in the long run, not only to our overall system of justice, but also within the daily operations of court dockets as these same bad government actors are no doubt currently involved in other cases.

A summary of the experts' findings follows.

⁵ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4928:3-7.

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

⁷ Dr. James Richard Kiper, Ph. D; Steven M. Abrams, J.D., M.S.; and Wayne B. Norris

⁸ *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.

II. ANOMALIES WITH SEARCH & 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 townhouse Mr. Raniere sometimes used, FBI agents entered the premises, completely bypassed the entrance, skipped the entirety of the downstairs area, went immediately upstairs, bypassed several more areas, and 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 and under the desk right next to the camera that were later seized, but they 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, which was later marked evidence item #2.

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 two other hard drives, which were later marked as evidence items #36 and #37.⁹ 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***.

[*This section intentionally blank to accommodate Figure B., next page.*]

⁹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4297:2-4311:5; Government Trial Exhibit 502A, hereafter "GX 502A," at GX 502A-32 & 33.

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.

II. Anomalies with Search and Evidence Handling



Figure: B.¹⁰

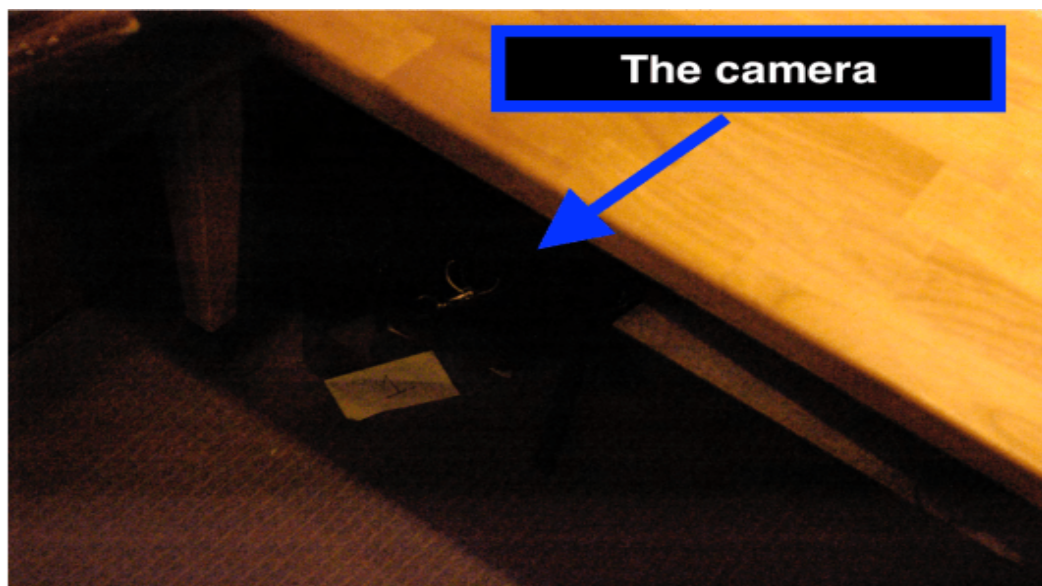


Figure: C.¹¹

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

¹¹ *Id.* at GX 502A-32.

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.

II. Anomalies with Search and Evidence Handling



Figure: D.¹²

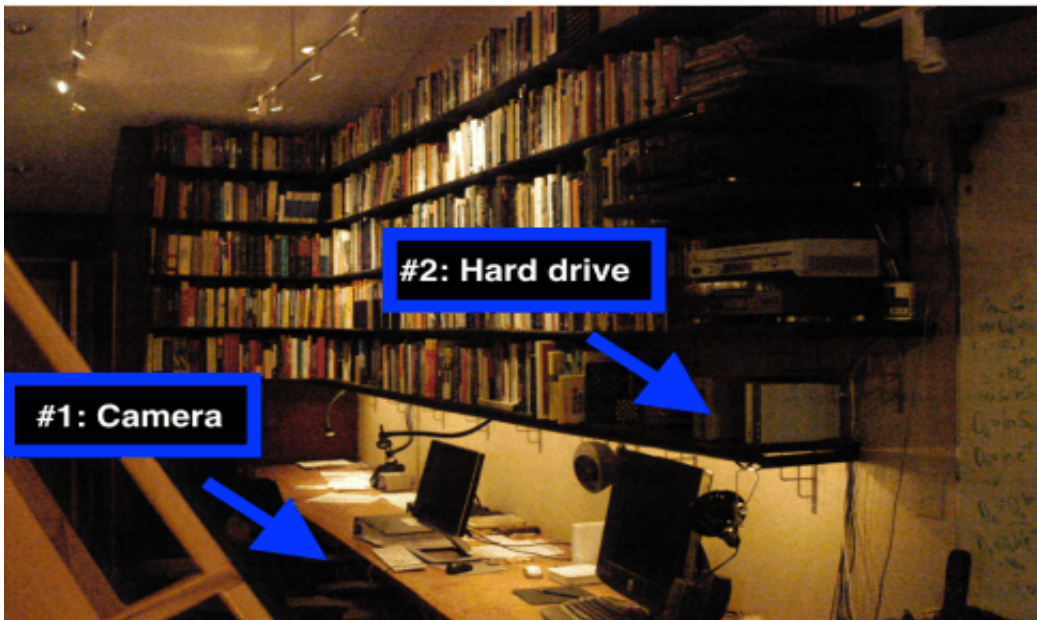


Figure: E.¹³

¹² *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) GX 502A-45; see also *Id.* at 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**].

¹³ *Id.* at 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.

II. Anomalies with Search and Evidence Handling

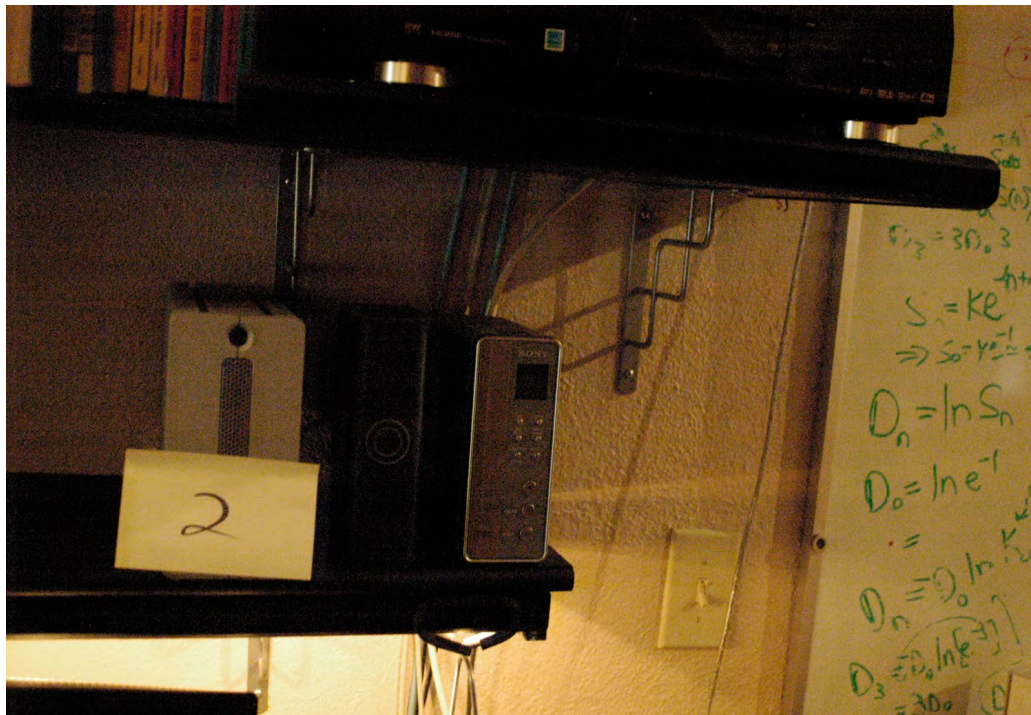


Figure: F¹⁴ Hard drive containing the 22 photos in the middle of two other hard drives.

¹⁴ *United States v. Raniere*, 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.

III. ANOMALIES WITH EVIDENCE COLLECTION, PROCESSING, & 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."¹⁵ 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.¹⁶

- On April 4, 2018, SA Lever checked the **hard drive**, the camera, and its **camera card** into Evidence Control.¹⁷ This was done according to FBI policy, which requires evidence to be checked into a secure location, such as Evidence Control, within 10 days of it being seized.¹⁸
- On July 10, 2018, SA Maegan Rees checked out the camera and **camera card** for "evidence review."¹⁹

FBI protocol **strictly prohibits** case agents from checking out and reviewing digital devices before the devices are processed by a forensic examiner in a CART forensic lab.²⁰ In processing, a CART forensic examiner will make a forensic image - an exact copy of a device in the identical state as when it was found at the scene. From there, only the forensic image (exact copy) will be examined and not the original device.²¹ 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 (exact copy).

- On July 27, 2018, SA Rees returned the camera and **camera card** back to Evidence Control.²²

¹⁵ *United States v. Raniere*, 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.

¹⁶ *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) 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.

¹⁷ *Id.* at DX 945; DX 960.

¹⁸ *Id.* at Dkt. 1169-1 at Ex. A at 15.

¹⁹ *Id.* at DX 945.

²⁰ *Id.* at Dkt. 1169-1 at Ex. C at 21.

²¹ *Id.* at Trial Tr. at 4781:3-4782:3.

²² *Id.* at DX 945 at 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.

III. Anomalies with Evidence Collection, Processing, & Analysis

- 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.”²³
- On September 19, 2018, SA Lever checked out the camera and **camera card** for “evidence review.” During this “check out,” which also violated FBI policy, the **camera card** was improperly and irreparably modified.²⁴
- Also on September 19, 2018, FET Donnelly forensically imaged (made an exact copy of) the **hard drive**.²⁵
- On September 24, 2018, FET Donnelly processed the **hard drive**.²⁶
- On September 26, 2018, at 11:45 a.m., SA Lever checked the **hard drive** out of Evidence Control. Twenty minutes later, at 12:05 p.m., he checked the **hard drive** into storage.²⁷ At 1:15 p.m., after having it in his possession for a week, he returned the **camera card** to Evidence Control.²⁸
- On October 3, 2018, FET Donnelly notified SA Lever that the **hard drive** was available on the secure network platform called, “Case Agent Investigative Review” hereafter “CAIR.”²⁹ Thus, while SA Lever was prohibited from directly analyzing the hard drive,³⁰ he could look through the forensic image (exact copy) by logging onto CAIR.
- On February 21, 2019, SA Lever ‘accidentally discovered’ the 22 alleged contraband photos reviewing the forensic image (exact copy) of the hard drive using the CAIR system.³¹
- On February 22, 2019, SA Lever checked the **hard drive** out of storage for search warrant purposes.³² This is yet another violation of FBI protocol, because he is prohibited from reviewing the actual item.³³ Further, SA

²³ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 001-004.

²⁴ *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.

²⁵ *Id.* at DX 961 at Bates 011.

²⁶ *Id.* at DX 961 at Bates 024.

²⁷ *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) at DX 960 at 2.

²⁸ *Id.* at DX 945 at 2.

²⁹ *Id.* at DX 961 at Bates 025.

³⁰ *Id.* at Dkt. 1169-1 at Ex. C at 21.

³¹ *Id.* at Dkt. 594-2 at ¶ 8 & 11 – Second Lever Aff; see also Dkt 618 at 2.

³² *Id.* at DX 960 at 3.

³³ *Id.* at 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.

III. Anomalies with Evidence Collection, Processing, & Analysis

Lever's physical possession of the hard drive here makes no sense; since October 3, 2018, *four and a half months*, he had been able to review the forensic image (exact copy) of the hard drive on CAIR, thus he had no need to possess the physical item that he is specifically barred from reviewing.

- Also on February 22, 2019, nearly two hours after SA Lever checked out the **hard drive**, he delivered the **camera card** to CART for the **first time**, turning it over to Senior Forensic Examiner, hereafter "SFE," Stephen Flatley."³⁴ The near two-hour overlap of the two devices being in SA Lever's sole possession is interesting to note.

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.³⁵ However, *because the CART lab had not yet forensically imaged the items*, FBI protocol specifically prohibited *any* review by *any* case agent.³⁶

- On April 11, 2019, SFE Brian Booth generated a forensic report for the **hard drive** based on FET Donnelly's processing.³⁷
- Also on April 11, 2019, SFE Flatley generated a forensic report for the **camera card** based on his own processing of it.³⁸

Importantly, these two reports offered only 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 183.³⁹

- On June 7, 2019, SA Lever made a request against FBI protocol⁴⁰ for SFE

³⁴ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) DX 945 at 3.

³⁵ *Id.* at Dkt. 1169-1 at Ex. C at 21.

³⁶ *Id.*

³⁷ *Id.* at DX 961 at Bates 028.

³⁸ *Id.* at GX 521A – Forensic Report of the Camera Card by SFE Stephen SFE Flatley (4/11/2019).

³⁹ *Id.* at Dkt. 1169-1 at Ex. D at Bates 028, Appendix D, Introduction.

⁴⁰ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) 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>”].

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.

III. Anomalies with Evidence Collection, Processing, & Analysis

- 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 reassignment to Ghana, Africa just six days before he was set to testify about the **camera card**.⁴¹ 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, 2019.⁴² However, instead of SFE Flatley giving the **camera card** directly to SFE Booth, who worked in the same CART lab, the camera and **camera card** were transferred to SA Elliot McGinnis.

- Also on June 7, 2019, SFE Flatley transferred the camera and **camera card** from CART to SA McGinnis.⁴³
- On June 10, 2019, at 10:02 a.m., SA Christopher Mills received the camera and **camera card** from SA McGinnis. He then testified in court the items⁴⁴ before giving them to SFE Booth at 4:55 p.m.⁴⁵
- On June 11, 2019, SFE Booth created a second forensic image of the **camera card** and generated a second forensic report.

This second forensic image, and corresponding second forensic report, were generated by SFE Booth during the last week of trial *without getting proper authorization*.⁴⁶ This June 11, 2019, report incredibly showed 37 *new* files which were *not present* in SFE Flatley's previous report from April 11, 2019.⁴⁷ This new **camera card** report, in contrast to SFE Flatley's report, now offered strong support for the government's theory as there were 31 additional photo files on the new report which matched files on the **hard drive**, bringing the total matching photo files between the **camera card** and **hard drive** to 35.⁴⁸

⁴¹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4987:1-16; see also DX 961 at Bates 029.

⁴² *Id.* at DX 945.

⁴³ *Id.*

⁴⁴ *Id.* at 4287:20-4314:23

⁴⁵ *Id.* at DX 945.

⁴⁶ *Id.* at Dkt. 1169-1 at Ex. D at Bates 029, Appendix D.

⁴⁷ *Id.*

⁴⁸ *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 029, Appendix D.

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.

IV. ANOMALIES ON THE HARD DRIVE

The hard drive that contained the 22 photos of alleged child pornography was an external hard drive that had alleged backup 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. Raniero, 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.⁴⁹ and Steven Abrams, who worked extensively with law enforcement including the United States Secret Service,⁵⁰ 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. Raniero was framed.

A. The Backup Itself

The hard drive appeared as if someone had used it to back up files from three different computers.⁵¹ 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." The aberrant backup contained seemingly common folders called, "My DVD's," "My Music," "My Pictures," "Studies," and "Symantec," but 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 suspiciously occurred in two steps. In the first step, only the "Studies" folder 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.⁵² Since the folders in this second step were practically empty, it does not make logical sense for anyone to make a separate effort to specifically back these up.

⁴⁹ *United States v. Raniero*, 18-cr-204-1 (NGG) (VMS) 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].

⁵⁰ *Id.* at Ex. E at Bates 001.

⁵¹ *Id.* at Dkt. 1169-1 at Ex. D at Bates 010, Finding 7; see also Trial Tr. at 4928:3-7.

⁵² *Id.* at 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. Raniero* (E.D.N.Y. 2019) 384 F. Supp. 3d 282.

IV. Anomalies on the Hard Drive

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 an automatic backup and then, 90 minutes later, adding the other empty folders and the music files to make the ‘backup’ appear more legitimate.

B. Folders and Subfolders

The “Studies” folder contained 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 a.m.⁵³ These folders appear to be computer-generated as users do not typically name folders after exact times down to the second.⁵⁴

These particular subfolders will be referred to as “DateTime” folders. The DateTime folder names roughly match the EXIF Creation dates of the photo files stored within. Thus, at first glance, it looks as if the photos were taken in 2005, and that, shortly after the photos were taken, someone downloaded the photo files to a 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 changed. Nevertheless, 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.⁵⁵

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 actually the result of manual manipulation.⁵⁶ Firstly, these subfolders could not have been generated by the Canon camera. The particular Canon camera model here 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.⁵⁷

Secondly, in evaluating between computer automation or manual manipulation, there are two anomalies that prove manual manipulation. The

⁵³ *United States v. Raniero*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4873:19 – 4874:4.

⁵⁴ *Id.* at Dkt. 1169-1 at Ex. D at Bates 008, Finding 6.

⁵⁵ *Id.* at Trial Tr. at 5371:16-24.

⁵⁶ *Id.* at Dkt. 1169-1 at Ex. D at Bates 008-009, Finding 6.

⁵⁷ *Id.*

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

IV. Anomalies on the Hard Drive

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 a.m. and 7:27:59 a.m., respectively, on October 19, 2005. DateTime folder 2005-10-19-0727-57 contained photo files 90-98. DateTime folder 2005-10-19-0727-59 contained photo files 79-89. However, for these times to be authentically created, a user would need to select photo files 90-98 from the camera, click an option in a program to download them to a computer, wait for them to fully download, then select photo files 79-89 from the camera, click to download them to the computer, and wait for them to fully download – all within two seconds. That is implausibly fast. More plausibly, someone named the folders manually but did not take the reality of user action time and actual file transfer time into account.⁵⁸

Thirdly, an anomaly was discovered in 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.⁵⁹

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 photo files, 79-89 and 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.⁶⁰

Thus, it is demonstrably provable 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 has not yet been 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

⁵⁸ *United States v. Ranieri*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 008-009, Finding 6.

⁵⁹ *Id.*

⁶⁰ *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.

IV. Anomalies on the Hard Drive

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.

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.

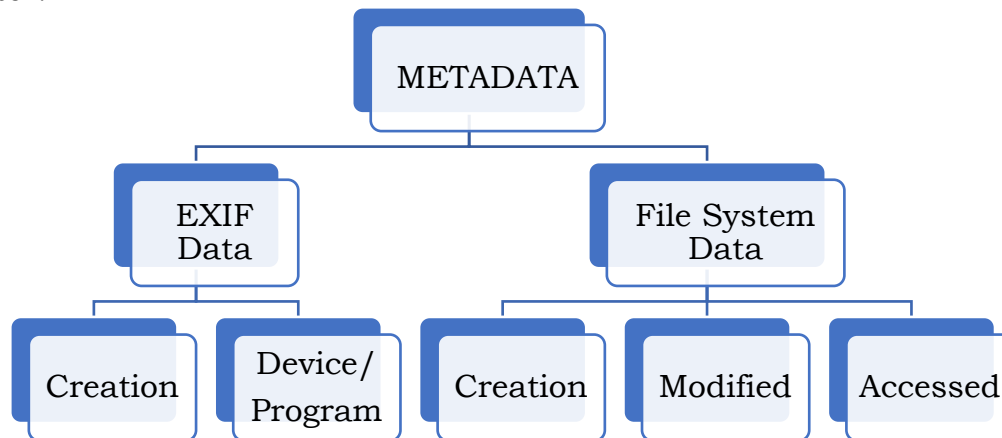


Figure A. *Hierarchy of Metadata types.*

An EXIF Creation date is the date set on a photo by the camera when taken.⁶¹ 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.⁶² 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, such as downloaded to a computer or backed up to a hard drive, the FS Creation date gets updated, whereas the EXIF Creation date will not change. However, the FS Creation date will not

⁶¹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D. at Bates 007 Finding 4.

⁶² *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.

IV. Anomalies on the Hard Drive

change if a photo is merely moved from one folder to another on the same device.

The FS Modified date is the date that marks the last time the photo was edited.⁶³ The initial FS Modified date will also be almost identical to the EXIF Creation date. The FS Modified date will not change unless the photograph is modified in some way, such as applying a filter or cropping it. The FS Modified date will not automatically change upon transfer to a new device.⁶⁴ 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 (1) reflect the new time zone or (2) 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 training module would be an FS Modified date. Lastly, the school would want one of their staff to periodically check in on the puppy to give it personal attention, to see and touch it, but not train it. This would be an FS Accessed date.

In summary for our hypothetical puppy, the birth certificate (EXIF Creation date) would always stay the same, unless someone tampered with it. If the puppy was ever sent to a different school, then for every new school the puppy was sent to, it would receive a new acceptance certificate (FS Creation date). For every training module the puppy completed, at any school, it would receive

⁶³ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D. at Bates 007 Finding 4.

⁶⁴ *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.

IV. Anomalies on the Hard Drive

a new training certificate (FS Modified date). Every time the puppy was seen and given personal attention but not training, such as play time, 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 interpreted differently when the file is copied, depending on the new computer's time zone settings.⁶⁵

Daylight Savings Time in 2005 occurred on Sunday, October 30, at 2:00 a.m.⁶⁶ Photo files 43 to 126 in the "Studies" folder have metadata that insinuates 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, at 2:00 a.m.⁶⁷

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.⁶⁸ 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 Pacific standard state which does not observe daylight savings, which is transferred to a school in California, a Pacific standard state which does observe daylight savings. The 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.⁶⁹ Then, on the same day, for photo files 138 to 149, their FS Modified dates **matched** their EXIF Creation

⁶⁵ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D. at Bates 007 Finding 4.

⁶⁶ 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>.

⁶⁷ *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Appendix B, at Bates 015 - 019.

⁶⁸ *Id.* at Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

⁶⁹ *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.

IV. Anomalies on the Hard Drive

dates.⁷⁰ 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.**⁷¹ 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.

Further, here, neither the Canon camera nor the camera card are able to store a time zone.⁷² 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,⁷³ 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 (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. 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.

⁷⁰ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

⁷¹ *Id.* at Dkt. 1169-1 at Ex. D at Bates 007 Finding 4.

⁷² Canon EOS 20D Digital Camera Manual at 34 (setting the date and time), found at <http://gd1p01.c-wss.com/gds/9/0900000259/01/EOS20DIM-EN.pdf>.

⁷³ 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%20automatic%20toggle%20button>.

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 the Hard Drive

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.⁷⁴

The alleged contraband photos on the hard drive are photo files 150 to 163 and 184 to 191.⁷⁵ Photo file 175 appears in the middle of these two ranges. Like the 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 it.**⁷⁶ 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.⁷⁷

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 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

⁷⁴ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007-08 Finding 5.

⁷⁵ *Id.* at Trial Tr. at 4875:24 - 4879:4.

⁷⁶ *Id.* at Dkt. 1169-1 at Ex. D at Bates 007-008, Finding 5.

⁷⁷ *Id.*

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.

IV. Anomalies on the Hard Drive

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.⁷⁸

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.”⁷⁹ However, inexplicably, their FS Modified dates are 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 for the CreatorTool was manually changed to zero to cover up the alterations.⁸⁰ The tamperer(s) merely made the mistake of leaving the EXIF CreatorTool value for photo file 175 set at “Photoshop Adobe Elements 3.0.”⁸¹

[*This section intentionally blank to accommodate Figure G., next page.*]

⁷⁸ *United States v. Raniero*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 007-08 Finding 5.

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ *Id.*

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.

IV. Anomalies on the Hard Drive

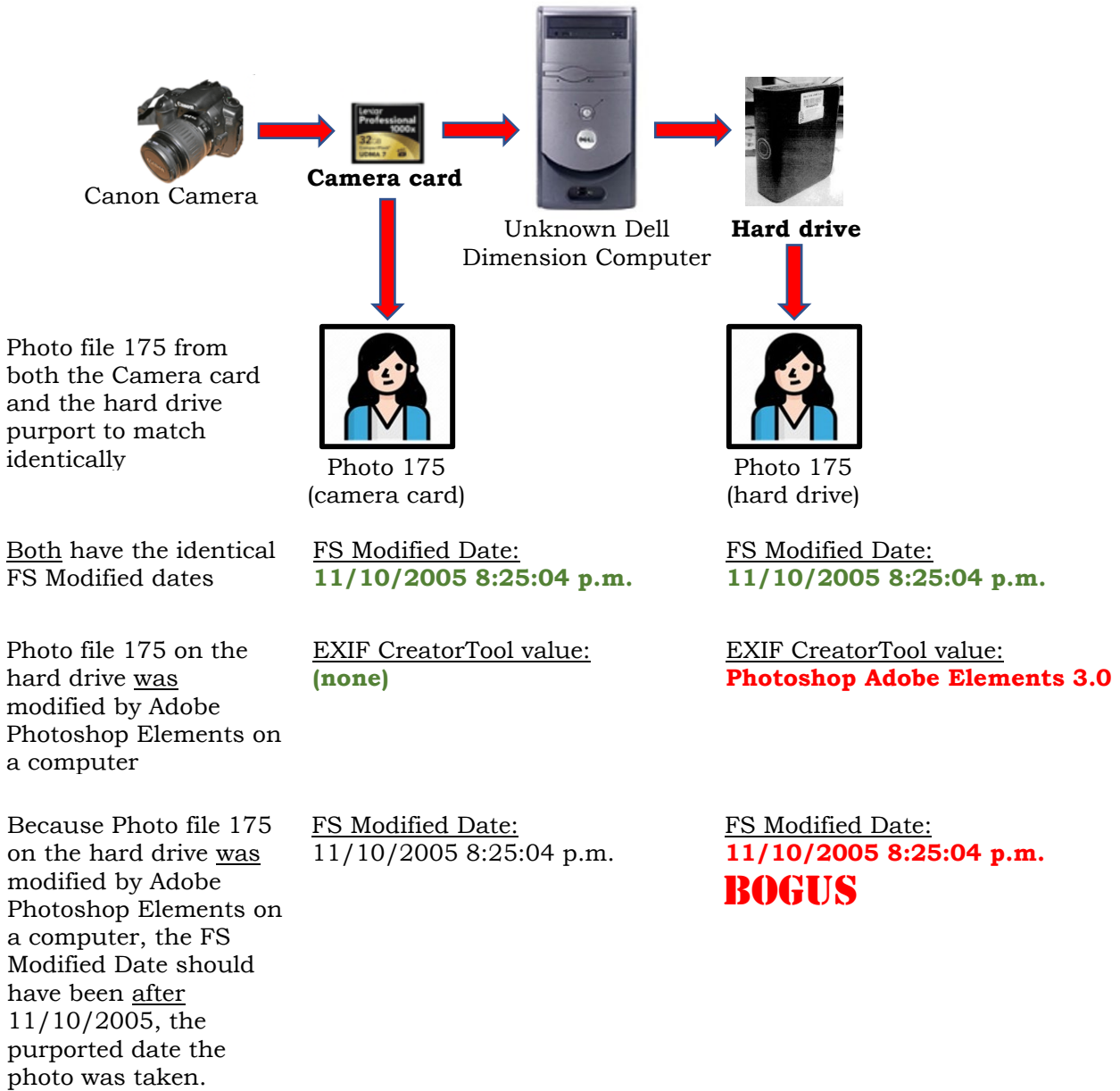


Figure G: Photo file 175 was altered on a computer but someone tried to cover that alteration up.

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 the Hard Drive

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

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. When files or folder are copied to a computer, FS Creation dates are updated to the current clock time of the receiving computer. For instance, if photo files with FS Creation dates of January 1, 2019, were copied from one computer to another on January 1, 2022, the copies would receive a new FS Creation date of January 1, 2022, updated from January 1, 2019. This is like a litter of puppies being transferred from their birth school to another school. All of the puppies within the transferred litter would get new acceptance certificates marked with the date and time that the new school received them.

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's clock *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.

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

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.

IV. Anomalies on the Hard Drive

not be updated.⁸² By analogy, the newly transferred puppies do not get new birth certificates or new training certificates just because they were accepted at a new school and received new acceptance certificates upon entry.




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

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.” According to its file listing, it came from the third, aberrant backup. The later part of the folder’s name, “20090330,” implies that the folder was created by an automatic backup that occurred on March 30, 2009.⁸³ Further, the folder’s metadata had an FS Creation date of March 30, 2009.⁸⁴ 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.

However, if one goes beyond this surface level of examination, and looks at the FS Creation dates for the photo files *within the folder*, one finds that **all the photo files in this entire backup folder have FS Creation dates of July 26, 2003.**⁸⁵

⁸² *United States v. Raniero*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 010-11 Finding 7.

⁸³ *Id.* at Dkt. 1169-1 at Ex. D at Bates 010-11 Finding 7; see also *Id.* at Trial Tr. at 4792:20-21.

⁸⁴ *Id.* at Dkt. 1169-1 at Ex. D at Bates 010, Finding 7.

⁸⁵ *Id.* at GX 505A.

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 the Hard Drive

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, 2005.⁸⁶ 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**.⁸⁷ Of course, this is impossible because one cannot back up a photo file two years before one has taken the photo. Moreover, the Canon camera in question was not manufactured until 2004.⁸⁸

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 appear 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, thus unknowingly giving all the photo 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, therefore leaving smoking gun evidence of tampering.

Finally, the backup folder 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.⁸⁹

⁸⁶ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Appendix B, Bates 015-217.

⁸⁷ *Id.* at Dkt. 1169-1 at Ex. D at Appendix B, Bates 015-217.

⁸⁸ DP Preview, Canon EOS 20D and preview (August 19, 2004) found at <https://www.dpreview.com/articles/1172584268/canon-eos20d>.

⁸⁹ *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.

V. ANOMALIES ON THE 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 35 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."⁹⁰ 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.

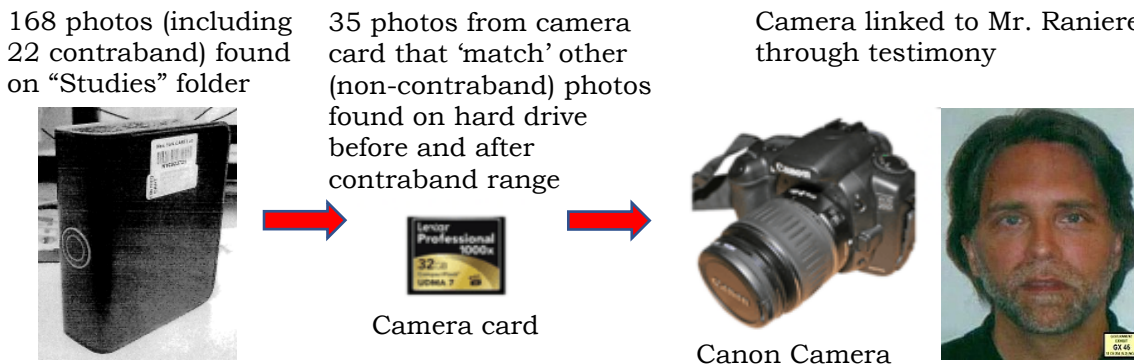


Figure J: Government's trial narrative linking Raniere to contraband photos.

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*.⁹¹ Regardless, 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, the entirety of the camera card and *any* evidence derived from it was not competent evidence.

⁹⁰ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 1536: 25 – 1537: 1; 2569; 2568: 24-25.

⁹¹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) 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.

V. Anomalies on the Camera Card

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

On September 19, 2018, FET Donnelly created a forensic image (exact copy) of the hard drive.⁹² 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 a forensic image has been made of the device by the CART lab.⁹³ Thus, SA Lever checked out an evidence item that neither he, nor any other agent, was authorized to view or inspect at the time.⁹⁴

On this same day, September 19, 2018, the camera card was improperly accessed without a write-blocker and was irrevocably altered.⁹⁵ 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.⁹⁶

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.⁹⁷ 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 FET Donnelly made a forensic image (exact 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.⁹⁸

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

⁹² *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) DX 961 at Bates 011; Bates 024.

⁹³ *Id.* at DX 945; See also Dkt. 1169-1 at Ex. C at 21.

⁹⁴ *Id.* at Ex. D at Bates 035, Finding 3.

⁹⁵ *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.

⁹⁶ *Id.* at Trial Tr. at 4781:5-19.

⁹⁷ *Id.* at Dkt 1169-1 at Ex. D at Bates 035, Finding 3 & 4.

⁹⁸ *Id.* at Dkt. 1169-1 at Ex. G – Search Warrant for 8 Hale Drive, Halfmoon, New York, issued March 26, 2018.

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.

V. Anomalies on the Camera Card

On April 11, 2019, SFE Flatley conducted a forensic examination of the camera card.⁹⁹ SFE Flatley, using the forensic examining software “AccessData Forensic Toolkit,” version 6.3.1.26, found 42 photos on the camera card.¹⁰⁰ 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).¹⁰¹ 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.

Two months later, on June 11, 2019, SFE Booth conducted a *second* forensic examination of the camera card.¹⁰² He used the same software, AccessData Forensic Toolkit, and the same version of the software, version 6.3.1.26, just as SFE Flatley had done. However, SFE Booth’s June 11, 2019, report incredibly found 37 *new* photos, of which 31 ‘matched’ photos on the hard drive.¹⁰³

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 unless specific authorization is obtained from the executive management of the FBI Operational Technology Division.¹⁰⁴ Nonetheless, on June 7, 2019, during the last few days of trial, SA Lever, against FBI policy,¹⁰⁵ requested SFE Booth to complete a new examination of and report on the camera card.¹⁰⁶

SA Lever requested this reexamination purportedly because SFE Flatley was going to be overseas and would therefore be unavailable to testify about his April 11, 2019, camera card report.¹⁰⁷ However, according to the FBI’s chain of custody log,¹⁰⁸ 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 had begun on May 7, 2019, SFE Flatley *had been available to testify at any time*

⁹⁹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) GX 521A – Forensic Report of Camera Card completed by SFE Flatley on April 11, 2019.

¹⁰⁰ *Id.*

¹⁰¹ *Id.*; see also *Id.* at Dkt. 1169-1 at Ex. D at Bates 028-029 Appendix D, Figure 1 & 2.

¹⁰² *Id.* at 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.”

¹⁰³ *Id.* at Dkt. 1169-1 Ex. D at Bates 028-32.

¹⁰⁴ *Id.* at Bates 037 Fn. 6.

¹⁰⁵ *Id.* at Ex. D at Bates 037 Fn. 6.

¹⁰⁶ *Id.* at DX 961 at Bates 029.

¹⁰⁷ *Id.*

¹⁰⁸ *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.

V. Anomalies on the Camera Card

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 card and *someone* therefore needed the camera card to be reexamined so these new files could appear in a new forensic report prior to SFE Booth testifying.

As noted, the FBI's forensic lab, CART, has a policy for reexaminations that require approval from the executive management of the FBI Operational Technology Division.¹⁰⁹ 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.¹¹⁰

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***.¹¹¹ Unbelievably, SFE Booth testified that he did not remember from whom he had received the evidence, though SA Mills had given it to him just two days prior.¹¹² This was on the fourth-to-last day of a trial that in total spanned 43 days. Further, *there is no record of who unsealed this evidence nor when 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.¹¹³ SFE Booth's examination notes¹¹⁴ end abruptly after he created the forensic image (exact 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.¹¹⁵

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

Four of the photo files that appeared for the first time on SFE Booth's June 11, 2019, report, 93, 94, 96, and 97, seem 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

¹⁰⁹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D at Bates 037 Fn. 6.

¹¹⁰ *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].

¹¹¹ *Id.* at Trial Tr. at 4889:14-18.

¹¹² *Id.* at Trial Tr. At 4889:7-13.

¹¹³ *Id.* at GX 521A Replacement; *See also Id.* at Trial Tr. at 4826: 6-17.

¹¹⁴ *Id.* at DX 961 at Bates 030.

¹¹⁵ *Id.* at Bates 030.

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.

V. Anomalies on the Camera Card

by the camera.¹¹⁶ 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 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.**¹¹⁷ On a normal backup, the camera card's photo files, including their thumbnails, would have counterparts on the hard drive that are identical matches. Computers do not make such errors; **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.¹¹⁸ Not only are they visually the same, but their MD5 Hash, or digital "fingerprints," are identical.¹¹⁹ Because photo files 180, 181, 182, and 183 were originally the *only* files in common between the hard drive and the camera card according to the April 11, 2019, camera card report and the April 11, 2019, hard drive report, this informs us how the tamperer(s) likely created the bogus photo files 93, 94, 96, and 97 – *and in all probability all 37 new photo files from the June 11, 2019, report*; since the hard drive had already been checked into evidence, forensically imaged (copied), examined in CART, and loaded into the CAIR system, the tamperer(s) did not have direct access to the hard drive and thus could not copy files directly from the hard drive to paste onto the camera card. Therefore, the safest way to reverse-engineer photo files to appear on the camera card that would have 'matches' on the hard drive, would be to replicate the four already existing proven matches – photo files 180-183. Hence, 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 changed 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.¹²⁰

Since the camera card was in the custody of the FBI during the time of the

¹¹⁶ *United States v. Raniere*, 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].

¹¹⁷ *Id.* at Dkt. 1169-1 at Ex. D at Bates 003, Finding 1.

¹¹⁸ *Id.* at Dkt. 1169-1 Ex. D at Bates 004, Finding 1.

¹¹⁹ *Id.* at Ex. D. at Bates 023-24.

¹²⁰ *Id.* at Ex. D at Bates 4, 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.

V. Anomalies on the Camera Card

appearance of these anomalies, and since these engineered 'matches' display limitations of someone having access to the hard drive's data but not the actual hard drive itself, *which during this time was the case with the involved FBI agents*, FBI agents are the only reasonable suspects for these anomalies.

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, 2019, camera card report. However, SFE Booth's report contains an additional 37 new photos.¹²¹ Accordingly, with the original four and the new 31 matching photos, the government now had a total of 35 photos from the camera card that 'matched' photos on the hard drive. This is significantly stronger evidence than the mere four matches that SFE Flatley had originally found.¹²²

Damningly, while the 42 photo files originally found by SFE Flatley were all viewable, **none** of the new 37 photo files found by SFE Booth were viewable.¹²³

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

As noted, before SFE Booth's June 11, 2019, camera card report, there were only four photo files in common between the camera card and the backup hard drive (180-183).¹²⁴ Eight of the newly appearing photo files (172-179) are located immediately before these common photo files. Next in the arrangement is a set of alleged contraband photos (184-191). After that, eight more of the newly appearing files (193-200) follow immediately after the alleged contraband range. The 'neat symmetry' of sixteen of the newly appearing photo files appearing directly before and after the alleged contraband photos fits the government's narrative precisely. Such newly appearing 'neat symmetry' in

¹²¹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Ex. D at Bates 028-32.

¹²² *Id.* at Ex. D at Bates 005, finding 2 at bp. 2; see also Bates 015-21, Appendix B.

¹²³ *Id.* at Dkt. 1169-1 Ex. D at Bates 005, Finding 2; Bates 028-29, Appendix D; Ex. E at Bates 003-02, Finding 1; Ex. F at Bates 004-005.

¹²⁴ *Id.* at Bates 028.

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.

V. Anomalies on the Camera Card

precisely the locations the government needed for its narrative is mathematically improbable and thus is more likely the result of tampering rather than coincidence.

Photo File #	
172	8 newly appearing photo files
173	
174	
175	
176	
177	
178	
179	
180	The only photos files initially in common between the camera card and the backup hard drive
181	
182	
183	
184	2 nd range of alleged contraband
185	
186	
187	
188	
189	
190	
191	
(192)	
193	8 more newly appearing photo files
194	
195	
196	
197	
198	
199	
200	

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

Moreover, there is another, telling example of this same 'neat symmetry' on SFE Booth's June 11, 2019, Camera Card Report which corroborates intentional placement as opposed to random photo taking behavior. Notably,

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.

V. Anomalies on the Camera Card

on the **hard drive**, under the "Studies" folder, there are three ranges of photos each with its own subfolder:

- Subfolder "MsK" ('Ms. Kathy') containing photo files 79-89
- Subfolder "Df" ('Daniela') containing photo files 90-98
- Subfolder "Mnp" ('Marianna and Pam') containing photo files 99-108¹²⁵

Suspiciously, only photo files 81 to 100 are among the newly appearing files on SFE Booth's June 11, 2019, **camera card** report.

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

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

¹²⁵ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) 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.

V. Anomalies on the Camera Card

Above, we see how photo files 79 and 80 from the 'Ms. Kathy' range, and photo files 101 to 108 from the 'Marianna and Pam' range are missing, leaving only the 'neat symmetry' of twenty photo files, 81-100, to appear on SFE Booth's June 11, 2019, **camera card** report which all too conveniently helped the government's narrative by increasing the matches between the **camera card** and the **hard drive** in the last days of the jury trial.

It is extremely unlikely that a normal camera user would have taken photos, saved them all to a hard drive and then gone back to the camera and deleted 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, then go back to the camera and delete only photos 79 and 80. Likewise with the range of Marianna and Pam photos, a normal camera user would not take exactly ten photos, photo files 99-108, back up all ten to a computer, and then go back to the camera and delete only the last eight photos, 101-108. In contrast, the range of Daniela has no photos deleted.

This behavior is inexplicable and would not be normal or reasonable behavior by a camera user. 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 SFE Booth's June 11, 2019, camera card report, thus bolstering the government's narrative at trial.¹²⁶

¹²⁶ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 Ex. D 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.

VI. PERJURY BY FBI SENIOR FORENSIC EXAMINER BRIAN BOOTH

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 for 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.¹²⁷ This testimony regarding the reliability of the 2005 dates bolstered the government's narrative that the 22 photos of Camila were contraband.¹²⁸ However, in actuality, EXIF data is quite easy to change, and anyone can do so on a home computer with no special skills or 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.¹²⁹ 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."**¹³⁰ SFE 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 mere days before he would have otherwise testified. *Someone* in the government, or some group of people, 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**

¹²⁷ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4818:24-4820:20, 4830:3-11, 4977:11-14.

¹²⁸ *Id.* at Trial Tr. at 5371:16-24; 5571:13-5572:3.

¹²⁹ *Id.* at Ex. D at Bates 042-046, Modifying Photograph EXIF Data.

¹³⁰ *United States v. Hirst*, 15-cr-643 (PKC) Dkt. 316 – Trial Transcript (September 20, 2016) hereafter "Hirst Trial Tr.," at 939:15-18; 941:6-12 [emphasis added]; see also Exhibit B attached herewith – Flatley versus Booth: An Analysis of Conflicting FBI Testimony Regarding EXIF Data by former FBI Special Agent by J. Richard Kiper, PhD, PMP.

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.

VI. Perjury by FBI Senior Forensic Examiner Brian Booth

the heart of our racketeering conspiracy." Without the racketeering charges, the government would have faced substantial venue, jurisdiction, and statute of limitations issues.

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 opened or unsealed the evidence.¹³¹ However, in actuality, physical evidence to be admitted into court must have a clear chain of custody establishing that it was not altered. As part of this process, evidence must be sealed as a rule and there must be clear documentation when it is unsealed as to who did so and why.¹³² 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 SFE Flatley's prior camera card report such that 37 new *and defective* files appeared on SFE 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, accordingly, we have a mountain of evidence evincing 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 also testified that there was no need to create a chain-of-custody log every time an evidence item is opened.¹³³ However, as noted above, this statement is demonstrably false; anytime sealed evidence is opened, there needs to be a log recording the opening of the evidence item.¹³⁴ 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.

¹³¹ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4886:15-4887:23.

¹³² *Id.* at Dkt. 1169-1 at Ex. D at Bates 033-035, Finding 1.

¹³³ *Id.* at Trial Tr. at 4887:21-4888:4.

¹³⁴ *Id.* at Dkt. 1169-1 at Ex. D at Bates 035, Finding 5.

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.

VII. PROSECUTORIAL ANOMALIES

As early as September 13, 2018, one of the lead prosecutors in this case, AUSA Moira 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, 2018.¹³⁵ 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.”¹³⁶ However, as previously noted, the FBI did not allegedly discover the contraband photos until February 21, 2019,¹³⁷ *44 days after AUSA Penza’s 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 newly discovered contraband photos, this raises the colloquial standard of, ‘What did Ms. Penza know and when did she know it?’

AUSA Penza’s uncanny precognitive statements to the court months before the alleged contraband photos were discovered, are eyebrow raising, especially in light of the multitude of irrefutable and expert-validated proof of government tampering presented in this document.

¹³⁵ *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Scheduling Conference Transcript (September 13, 2018), at 13: 24 -14: 8.

¹³⁶ *Id.* at Motion Hearing Transcript (January 9, 2019) hereafter “Mot Tr., (1/9/18)” at 4:4-25.

¹³⁷ *Id.* at Dkt. 594-2 – Second Lever Aff at ¶ 8 & 11 (filed under seal); See also Dkt 618 at 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.

VIII. 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 these findings 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 correct an injustice as well as prevent further injustices.

Not only is there a manifest injustice each second that Mr. Raniere continues to spend behind bars based on false and manipulated evidence, but there should also be no doubt that the bad actors within government who perpetrated this planting, manufacturing, and tampering of evidence, continue to work on and be involved with other active cases. Whether or not these bad government actors are engaging in the same criminal conduct on other cases, 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 reexamined *in all other cases in which they were allowed to work*. This will impact many other Accused individuals, as well as many other cases in which any potential bad governmental actors are involved. This, in turn, will negatively impact court dockets and thus the functioning of the court system at large. 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.

Exhibit B

Affidavit of Dr. James Richard Kiper, Ph.D.

State of Florida
County of Leon

COMES NOW Dr. James Richard Kiper, Ph.D., being first duly sworn, under oath, and states that the contents of the following attached report(s), including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Flatley versus Booth: An Analysis of Conflicting FBI Testimony Regarding EXIF Data

Signature: 

Address: 818 Shannon Street
Tallahassee, Florida 32305

SUBSCRIBED AND SWORN TO before me this 6th day of Sept., 2022, by

James R. Kiper

Physically appeared
and attested before me.


NOTARY PUBLIC FOR FLORIDA



DOUGLAS E WRIGHT
Commission # GG 293252
Expires March 22, 2023
Bonded Thru Budget Notary Services

My Commission Expires: 3-22-23

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

September 5, 2022

Flatley versus Booth: An Analysis of Conflicting FBI Testimony Regarding EXIF Data

Professional Background

I 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. In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally sworn out affidavits for dozens of search warrants and collected, preserved, and analyzed hundreds of pieces of digital evidence. Therefore, I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

Introduction

In the case *U.S. vs KEITH RANIERE, et al.* the government contended that Raniere used a digital camera to take explicit photographs of women, saved them to a camera card, transferred them to an unidentified computer, and then backed them up to an external hard drive. The camera card and the “backup” hard drive comprised the only digital evidence used at trial. According to the government’s narrative, all the backed-up photographs were taken in the year 2005, at a time when one of the women was 15 years old. **The government argued if the pictures were taken in 2005, then 22 photos of the backed-up photos would constitute child pornography.**

In order to date these photographs, the government relied on two pieces of digital information – the names of the folders containing the photos and the “Create Date,” saved inside the content portion of the photo called EXIF data. The problem is that both pieces of data are forensically unreliable. Any computer user who has created a folder realizes how easy it is to modify a folder name. And while fewer people know how to modify the embedded “Create Date” in a photo’s EXIF data, I have conclusively demonstrated the ease of modifying this data using Windows functionality with no special skills or tools.¹ Nevertheless, the government insisted that EXIF data is “hard to change” and “is extremely reliable.”²

¹ See my Summary of Process Findings report, Appendix A for a full demonstration and debunking the government’s claim that EXIF data is “very hard to modify,” found at *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.

² *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Transcript hereafter, “Trial Tr.,” at p.4977; 5572.

Senior Forensic Examiner (SFE) Brian Booth was the FBI's expert witness who testified under oath as to the reliability of EXIF data. He did so after being requested to conduct a *second forensic examination* of the camera card, which he had received in an unsealed package during the final days of the trial.³ SFE Booth produced a "replacement" forensic report of the camera card on 06/11/2019, and it contained 37 additional files *not included in the first FBI forensic report*. Although 31 of the 37 new files had namesake counterparts on the alleged backup hard drive, the new files had several issues with *metadata* and showed dispositive evidence of manual alterations.⁴

SFE Stephen Flatley⁵ was the first forensic examiner to examine that camera card and had produced a report two months earlier, on 04/11/2019. However, the government declined to put SFE Flatley on the stand to explain his report. Instead, during the fifth and final week of trial the government abruptly gave SFE Flatley an overseas assignment and through the hands of several people transferred the camera card to SFE Booth in an unsealed package.

Until recently, the government's refusal to use SFE Flatley and his report during the first four weeks of trial was an inexplicable decision. However, I believe SFE Flatley's testimony on a *previous case* could shed some light on this mystery. As I will explain in the following pages, SFE Flatley's previous testimony *directly contradicted* SFE Booth's testimony regarding the reliability of metadata dates, and to be consistent SFE Flatley *likely would not have supported the government's claims* in U.S. vs KEITH RANIERE.

The 2016 Trial Testimony of SFE Stephen Flatley

On 09/20/2016, SFE Flatley was called to testify as the government's expert witness in the case U.S. vs GARY HIRST.⁶ After qualifying SFE Flatley as an expert witness, prosecutor Brian Blais immediately began questioning SFE Flatley on the topic of *metadata* and *dates*:

Q. Where is **metadata stored**?

A. There is two different places overall where it could be stored. It could be stored in the computer's file system in the computer itself. So the overall **creation date** of the file could be stored there. Certain files also have **metadata stored inside them**. Things like Word documents, **PDF documents**, some photographs, like **JPEGs** and a certain type called **JPEG Exif** will have certain other aspects of metadata inside of it.

Q. How is metadata generated?

A. It's generated at the time the file is created, and **then it can be modified** at later dates.⁷

³ See my Summary of Process Findings report for further details, found at *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.

⁴ See my Summary of Technical Findings, Finding's #1 and #2, found at *Id.*

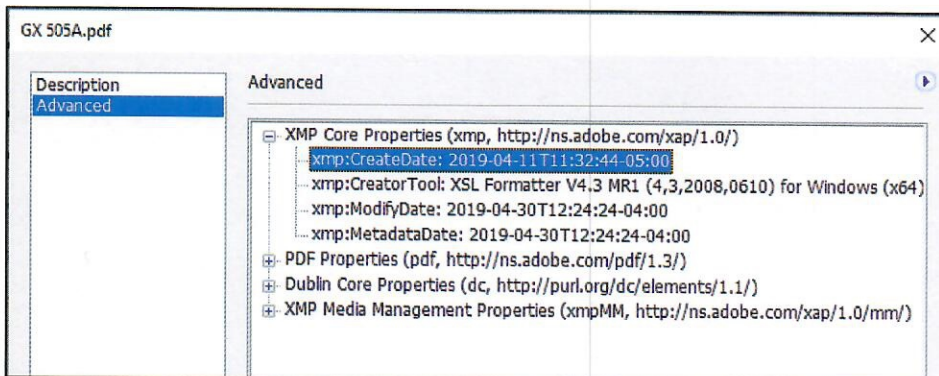
⁵ For full disclosure, I am acquainted with SFE Flatley personally and have co-instructed with him while serving as a digital forensics instructor in the FBI.

⁶ *United States v. Hirst*, 15-cr-643 (PKC) (SDNY Apr. 18, 2022).

⁷ *Id.* at Trial Transcript hereafter, "Trial Tr.," at p. 935:24-936:9.

During this exchange, it was appropriate for SFE Flatley to mention the similarity of metadata stored inside PDF documents with that stored inside JPEG (photo) files as EXIF data. Indeed, PDF files and JPEG files store “Create date” information in essentially the same way – by inserting the date and time into the content of the file.

To illustrate this fact, I opened the PDF document Government’s Exhibit “GX 505A.pdf,” representing the FBI’s forensic report of the external hard drive in this case. By clicking File > Properties > Additional Metadata I could view the imbedded “Create Date” of the document as 04/11/2019.



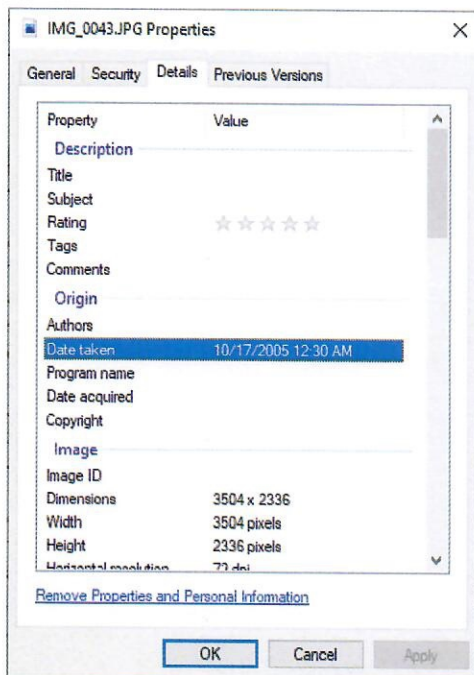
Using a forensic tool, FTK Imager, I verified that the date is indeed part of the *content* of the file, rather than stored elsewhere in the file system, by opening the same GX 505A.pdf document and viewing the hexadecimal representation of the data:

Name	Size	Type	Date Modified
GX 505A.pdf	4,808	Regular File	5/12/2021 10:30:58 PM
GX 521A.pdf	306	Regular File	5/12/2021 10:30:50 PM
GX 521A_Replacement.pdf	1,127	Regular File	5/12/2021 10:30:56 PM
GX 527.csv	2	Regular File	5/12/2021 10:30:50 PM
GX 550 - File List 2.pdf	356	Regular File	5/12/2021 10:30:52 PM

4a1400	65 2E 63 6F 6D 2F 70 64-66 2F 31 2E 33 2F 22 0A	e.com/pdf/1.3/"
4a1410	20 20 20 20 20 20 20 20-20 20 20 20 78 6D 6C 6E	xmlns
4a1420	73 3A 64 63 3D 22 68 74-74 70 3A 2F 2F 70 75 72	s:dc="http://pur
4a1430	6C 2E 6F 72 67 2F 64 63-2F 65 6C 65 6D 65 6E 74	l.org/dc/element
4a1440	73 2F 31 2E 31 2F 22 0A-20 20 20 20 20 20 20 20	s/1.1/"
4a1450	20 20 20 20 78 6D 6C 6E-73 3A 78 6D 70 4D 4D 3D	xmlns:xmpMM=
4a1460	22 68 74 74 70 3A 2F 2F-6E 73 2E 61 64 6F 62 65	"http://ns.adobe
4a1470	2E 63 6F 6D 2F 78 61 70-2F 31 2E 30 2F 6D 6D 2F	.com/xap/1.0/mm/
4a1480	22 3E 0A 20 20 20 20 20-20 20 20 3C 78 6D 70	">
4a1490	3A 43 72 65 61 74 65 44-61 74 65 3E 32 30 31 39	<xmp
4a14a0	2D 30 34 2D 31 31 54 31-31 3A 33 32 3A 34 34 2D	CreateDate>2019
4a14b0	30 35 3A 30 30 3C 2F 78-6D 70 3A 43 72 65 61 74	-04-11T11:32:44
4a14c0	65 44 61 74 65 3E 0A 20-20 20 20 20 20 20 20 20	05:00</xmp:Creat
4a14d0	3C 78 6D 70 3A 43 72 65-61 74 6F 72 54 6F 6F 6C	eDate>
4a14e0	3E 58 53 4C 20 46 6F 72-6D 61 74 74 65 72 20 56	<xmp:CreatorTool
4a14f0	34 2E 33 20 4D 52 31 20-28 34 2C 33 2C 32 30 30	>XSL Formatter V
4a1500	38 2C 30 36 31 30 29 20-66 6F 72 20 57 69 6E 64	4.3 MR1 (4,3,200
4a1510	6F 77 73 20 28 78 36 34-29 3C 2F 78 6D 70 3A 43	8,0610) for Wind
4a1520	72 65 61 74 6F 72 54 6F-6F 6C 3E 0A 20 20 20 20	ows (x64)</xmp:C
4a1530	20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20	reatorTool>
		<xmp:Modif

Using these two screen shots, one can observe the imbedded date/time of “04/11/2019 11:32:44” is saved as the “Create Date” value inside the content of the “GX 505A.pdf” file. This is exactly what SFE Flatley was describing during his testimony.

As SFE Flatley mentioned during his testimony, JPEG photo files also contains metadata, stored essentially in the same way, inside the content of the file as EXIF data. In the following screen shot I viewed the properties of “IMG_0043.JPG,” a JPEG photo file in this case. The EXIF create date is displayed as “10/17/2005 12:30AM” which is interpreted by Windows as “Date taken.”



Loading this file into another program, Exiftool, one observes the name of metadata create date of the JPEG is identical to that of the PDF, which is “Create Date”:

```
C:\Photos>exiftool ./Originals/IMG_0043.JPG |find "Date"
File Modification Date/Time      : 2005:10:16 23:30:04-04:00
File Access Date/Time           : 2022:09:01 14:09:31-04:00
File Creation Date/Time         : 2022:02:28 13:48:56-05:00
Modify Date                     : 2005:10:17 00:30:04
Date/Time Original              : 2005:10:17 00:30:04
Create Date                     : 2005:10:17 00:30:04
```

Using the same procedure used for the PDF document, I opened the JPEG file using FTK Imager and verified the date in the *content* of the photo file:

File List			
Name	Size	Type	Date Modified
IMG_0043.JPG	4,183	Regular File	10/17/2005 3:30:04 AM
IMG_0044.JPG	2,232	Regular File	10/17/2005 7:53:24 PM
IMG_0045.JPG	2,488	Regular File	10/17/2005 7:53:40 PM
IMG_0046.JPG	2,244	Regular File	10/17/2005 7:54:08 PM
IMG_0047.JPG	2,198	Regular File	10/17/2005 7:54:24 PM
IMG_0048.JPG	1,027	Regular File	10/17/2005 7:54:38 PM
000000	FF D8 FF E1 4F 93 45 78-69 66 00 00 49 49 2A 00		ÿØÿàO-Exif-·II*
000010	08 00 00 00 09 00 0F 01-02 00 06 00 00 00 7A 00	z.
000020	00 00 10 01 02 00 0E 00-00 00 80 00 00 00 12 01	
000030	03 00 01 00 00 00 01 00-33 33 1A 01 05 00 01 00	33.....
000040	00 00 A0 00 00 00 1B 01-05 00 01 00 00 00 A8 00	
000050	00 00 28 01 03 00 01 00-00 00 02 00 CC CC 32 01		..(.....iî2.
000060	02 00 14 00 00 00 B0 00-00 00 13 02 03 00 01 00	*
000070	00 00 02 00 32 20 69 87-04 00 01 00 00 00 C4 00		...2 i.....Ä.
000080	00 00 58 24 00 00 43 61-6E 6F 6E 00 43 61 6E 6F		·Xÿ·Canon·Cano
000090	6E 20 45 4F 53 20 32 30-44 00 40 00 CC 8C 40 8C		n EOS 20D·@·I·@·
0000a0	CC CC C0 04 C4 CC 00 04-33 33 11 20 48 00 00 00		iîÄ·Äî·33·H...
0000b0	01 00 00 00 48 00 00 00-01 00 00 00 32 30 30 35		...H.....2005
0000c0	3A 31 30 3A 31 37 20 30-30 3A 33 30 3A 30 34 00		:10:17 00:30:04-
0000d0	1C 00 9A 82 05 00 01 00-00 00 1A 02 00 00 9D 82	
0000e0	05 00 01 00 00 00 22 02-00 00 22 88 03 00 01 00	"....."
0000f0	00 00 02 00 00 33 27 88-03 00 01 00 00 00 64 00	3'.....d.
000100	33 33 00 90 07 00 04 00-00 00 30 32 32 31 03 90		33.....0221...
000110	02 00 14 00 00 00 2A 02-00 00 04 90 02 00 14 00	*

Although the majority of SFE Flatley’s testimony addressed metadata embedded inside PDF documents, he immediately drew a similarity to metadata inside of JPEG photo files. Indeed, as the above exercise demonstrates, they are essentially created and stored in the same way.

More importantly, SFE Flatley stated *another aspect* of metadata in the transcript excerpt cited above. Immediately after mentioning JPEG EXIF data, SFE Flatley revealed that metadata stored inside of files “**can be modified at later dates.**” How? SFE Flatley testified that Exiftool and Xpdf, two freely available software tools, may be used to modify metadata in JPEG and PDF files. In fact, with respect to these publicly available metadata authoring tools, SFE Flatley testified, “[T]here’s a bunch of them.”⁸ How would a person obtain such a tool? SFE Flatley testified, “You just download it from the web.”⁹

The Unreliability of Embedded Metadata Dates

Because their determination of *child pornography* solely depended on the *created dates of the photographs*, the FBI’s expert witness SFE Booth and DOJ’s prosecutor Tanya Hajjar went to great lengths to convince the jury of the reliability of EXIF data. What follows are just a few statements from their exchanges during trial (emphasis added):

- Q. Is there a particular reason why **EXIF** data is **more difficult** to alter?
- A. They purposely designed it that way.
- Q. Do you know --

⁸ *Hirst, supra*, 15-cr-643 (PKC) Trial Tr. at p.936:17-21.
⁹ *Id.* at p.941:22-942:3.

A. It's mainly to be able to store information. And they don't want data to be moved around and changed, **especially time and date information**. Those things are **very hard for the consumer to be able to modify**, unless you wind up getting **software** that's just developed to do that¹⁰

Later in his testimony, SFE Booth admitted that the *file system* Created date for all the “backed up” photos, including the alleged contraband, was in 2003. This would mean the photos were copied to the external hard drive *two years before* the government claimed they were taken – a physical impossibility. Therefore, after recognizing they could not rely on the *file system* create dates for the backup files¹¹, SFE Booth and prosecutor Hajjar turned their attention back to the easily-modifiable *EXIF data* to support the create date they needed the jury to believe.

Q. You testified that the EXIF data shows the date and time associated with this is October 18, 2005?

A. Yes.

Q. And so between the dates here and the EXIF data, what's the **best evidence** of when this photograph was taken?

A. Well, the best reference is the **EXIF** data because that gets put into the JPEG file and it's **not easily modifiable** and it moves with the file the same way from device to device, no matter where you place it. It has nothing to do with the bearing of a file system at all or the dates and times associated with it. So it's on its own, but are created at the same time that you take the picture¹²

These are just a few of SFE Booth's statements regarding the reliability of EXIF data and how difficult it is to modify. The court transcript records *15 pages* of SFE Booth and prosecutor Hajjar mischaracterizing the reliability of EXIF metadata¹³. Again, to support their narrative that the alleged contraband photos were taken in 2005, the government needed the jury to believe the reliability of the metadata.

The reliability of the EXIF data was so crucial to the government's charge of child pornography, prosecutor Mark Lesko emphasized Booth's testimony during his closing argument to the jury:

LESKO: ...I'm no expert, don't get me wrong, **but I heard Examiner Booth, just like you did. Exif data is extremely reliable.** It's

¹⁰ *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Transcript hereafter, “Trial Tr.” at p. 4820:2-20.

¹¹ *Id.* at Trial Tr. at p. 4829:12-24 [emphasis added], From Booth's trial testimony: [“As you move things from one computer to another, if the times are different and they're different types of file systems, they'll get a new created time and if dates are wrong, they can be *manipulated*...Usually, if anything, it would be the created time that would be changed. Sometimes you can get a created dated that's after your modified date, which happens when you just happen to move to a different type of file system later on after you've had the file. But in this case, it's actually **reversed**. *Somehow it got changed to where the date is well, well, before then what might be the first modified date or a modified date.*”] On cross examination, SFE Booth openly admitted that the file creation dates for all the “backed up” photos, including the alleged contraband, were unreliable: “...The file system metadata for those dates and times are not accurate” *Id.* at Trial Tr. at p. 4941:1-19. Hence, to support the 2005 create date the government needed the jury to believe in the reliability of JPEG EXIF data.

¹² *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at p. 4829:25-4830:11.

¹³ *Id.* at Trial Tr. at p. 4816-4831.

embedded in the jpeg, in the image itself. And the exif data shows that the data was created on the camera, in this instance, this particular instance, the 150 jpeg on November 2, 2005...¹⁴

SFE Flatley, the FBI's expert witness in a previous trial, would disagree:

Q. Now, Mr. Flatley, does the FBI **rely on creation dates alone** in PDF files in determining the date on which that PDF file was, in fact, created?

A. **No, we do not do that.**¹⁵

Earlier in this paper, I demonstrated that PDF files and JPEG files use the same method for storing metadata for creation dates. In fact, PDF files and JPEG files even use the *same metadata tag*, "Create Date" to record this information. Since SFE Flatley discussed the composition of JPEG files alongside PDF files in his testimony, he would similarly testify that the FBI does NOT rely on creation dates alone in determining the date on which a JPEG file was created.

Why not? According to SFE Flatley, the FBI "would require that we have some kind of corroborating evidence."¹⁶ To rely upon the metadata "Create Date" in either a PDF or JPEG file, the FBI would require corroborating data from other devices and mechanisms that possibly stored or transmitted the file, but these devices must be "outside the user's control."

A. So something that was not just from the standalone system that would require some kind of corroboration or something outside the user's control.¹⁷

Despite SFE Flatley's claim to the contrary, in the case U.S. vs KEITH RANIERE, the FBI used no other devices, systems, or mechanisms to corroborate the easily-modifiable EXIF metadata dates in the JPEG files. Instead, the FBI consistently claimed EXIF metadata was reliable by itself and difficult to change, as SFE Booth testified on cross examination:

A. ...But when it comes to photos, they still keep you from changing **dates** and **times**. **It's not easy to change those**. You have to go through **special processes** to change those things.¹⁸

By contrast, SFE Flatley gave a very different answer when asked for reasons why a create date "reflected in the file's metadata may not match the actual creation date." SFE Flatley testified to several reasons why file metadata dates are unreliable:

¹⁴ *Ranieri, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at p. 5572.

¹⁵ *Hirst, supra*, 15-cr-643 (PKC) Trial Tr. at p.939:15-18.

¹⁶ *Id. at* Trial Tr. at p.940:9-23.

¹⁷ *Id.*

¹⁸ *Ranieri, supra*, 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4977:11-14.

A. A computer's clock is too easily changed. It's very easy to go down and change your time and date on the machine. It's also a standalone system. It could just flat be wrong. The clock could be off, it could have been changed either inadvertently or by, what's the word I'm thinking of, just, you know, just out of habit or something of that nature that they just change the time, date. Also, your machine, when it's off, relies on a battery to keep the clock up. It's called the cmos battery. If that battery dies, the clock will revert to its beginning.¹⁹

Just as SFE Booth repeatedly testified that the FBI considered metadata create dates *reliable*, SFE Flatley repeatedly testified that the FBI considered metadata create dates *unreliable*:

Q. Based on your training and experience, would the FBI **rely** on the **create dates alone** in the metadata of Government's Exhibits 509A through D in determining the dates on which these documents were created?

A. **No, we would not.**²⁰

SFE Flatley's position regarding the unreliability of metadata create dates was not an ancillary opinion – it was the entire purpose for his testimony. As the prosecutor concluded his direct examination:

Q. So Mr. Flatley, in your opinion, can you conclude that Government's Exhibits 509A through D were **created on the dates** reflected in the **metadata** in those documents?

A. **I cannot.**²¹

Conclusion

In the case U.S. vs KEITH RANIERE it is notable that SFE Flatley, an FBI expert witness who previously testified to the unreliability of metadata create dates, was *replaced* in the last week of trial by SFE Booth, who testified to the reliability of metadata create dates. And although the government did not allow SFE Flatley to testify in the RANIERE case, much of his prior testimony directly supports the findings in my Summary of Technical Findings report.²²

¹⁹ *Hirst, supra*, 15-cr-643 (PKC) Trial Tr. at p.941:6-15.

²⁰ *Id.* at Trial Tr. at p. 951:9-13.

²¹ *Id.* at Trial Tr. at p. 952:4-7.

²² In *United States v. Hirst*, SFE Flatley even testified about the impossibility of a file content being changed without its file system Modified date being updated. When asked about the Modified date, SFE Flatley said, "It reflects the last time that a change was made to that file and then that file was saved again. So if you were to change something in a file and then not save it, that date would not be touched. **But if you change anything on the file and then save it again, the modified dated will be altered.**" *Id.* at Trial Tr. at p. 942:22-945:2. This statement alone supports nearly all the findings of manual alterations in my Summary of Technical Findings report found at *Raniere, supra*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.

In addition to demonstrating elsewhere how easy it is to change metadata create dates²³, in this paper I forensically demonstrated that PDF files and JPEG files *name* and *store* the “Create Date” value in same way – inside the content of the file. In his 2016 testimony SFE Flatley not only argued strongly that metadata create dates are *unreliable*, but he also did not waver from this opinion or draw any distinction between metadata create dates in PDF files versus those in JPEG files.

Consider SFE Flatley’s expert opinions made under oath:

- SFE Flatley highlighted the similarity between metadata stored inside PDF files and metadata stored inside JPEG files.
- SFE Flatley described two different free tools anyone could use to modify metadata such as EXIF data.
- SFE Flatley declared such tools are easy to obtain from the Web.
- SFE Flatley declared on at least four occasions that metadata create dates are unreliable.
- SFE Flatley described several ways metadata create dates could be altered.
- SFE Flatley declared that the FBI in particular does not rely on metadata creation dates alone to determine when a file was, in fact, created.

To defend SFE Booth’s testimony against SFE Flatley’s testimony, one may argue that a PDF document is not the same as a JPEG photo. However, to discount SFE Flatley’s damning testimony about the unreliability of metadata create dates, one would need to prove that metadata stored inside the content of a JPEG photo file is somehow more reliable than the metadata stored inside the content of a PDF file. It is not. In fact, quite the opposite – It is much easier to modify the EXIF create date of a JPEG file.

Thus, in U.S. vs KEITH RANIERE, there is *no doubt* that the government mischaracterized the reliability of EXIF metadata during trial testimony. No doubt SFE Flatley would agree with that assessment, based on his past testimony, if he were given the opportunity to testify in this case.

Respectfully Submitted,



J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

²³ See my Summary of Process Findings report, Appendix A for a full demonstration and debunking the government’s claim that EXIF data is “very hard to modify.”

CERTIFICATE OF SERVICE

I hereby certify that, on October 6, 2022, a true and correct copy of the DEFENDANT-APPELLANT MOTION TO HOLD CASE IN ABEYANCE was filed and served electronically through the Court's CM/ECF system upon the following counsel of record:

Tanya Hajjar, Esq.
Direct: 718-254-6109
[COR LD NTC US Attorney]
United States Attorney's Office for the Eastern District of New York
271 Cadman Plaza East
Brooklyn, NY 11201

Kevin Trowel, Esq.
Direct: 718-254-6469
[COR NTC US Attorney]
United States Attorney's Office for the Eastern District of New York
271 Cadman Plaza East
Brooklyn, NY 11201

Ronald S. Sullivan, Jr., Esq., Professor
Direct: 617-496-4777
[COR LD NTC Retained]
Harvard Law School
Harvard Criminal Justice Institute
1585 Massachusetts Avenue
Cambridge, MA 02138

Daniel Rickert Koffmann, Esq.
Direct: 212-849-7617
[COR NTC Retained]
Quinn Emanuel Urquhart & Sullivan, L.L.P.
22nd Floor
51 Madison Avenue
New York, NY 10010

Dated: October 6, 2022.

Respectfully submitted,

/s/ Joseph M. Tully
Joseph M. Tully
(CA Bar. No. 201187)