Appendix 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.

Douglas E Wright
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 Flatley[5] 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*:

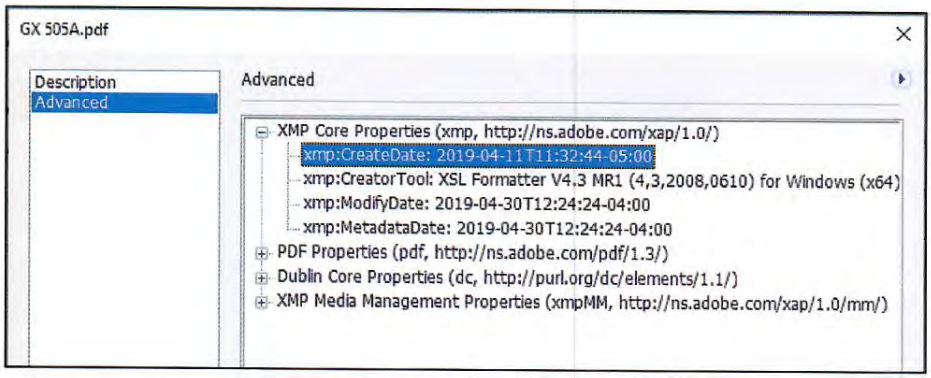
Q. Where is **metadata stored**?
A. There is two different places overall where it could be stored. It could be stored in the computer's file system in the computer itself. So the overall **creation date** of the file could be stored there. Certain files also have **metadata stored inside them.** Things 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]

---

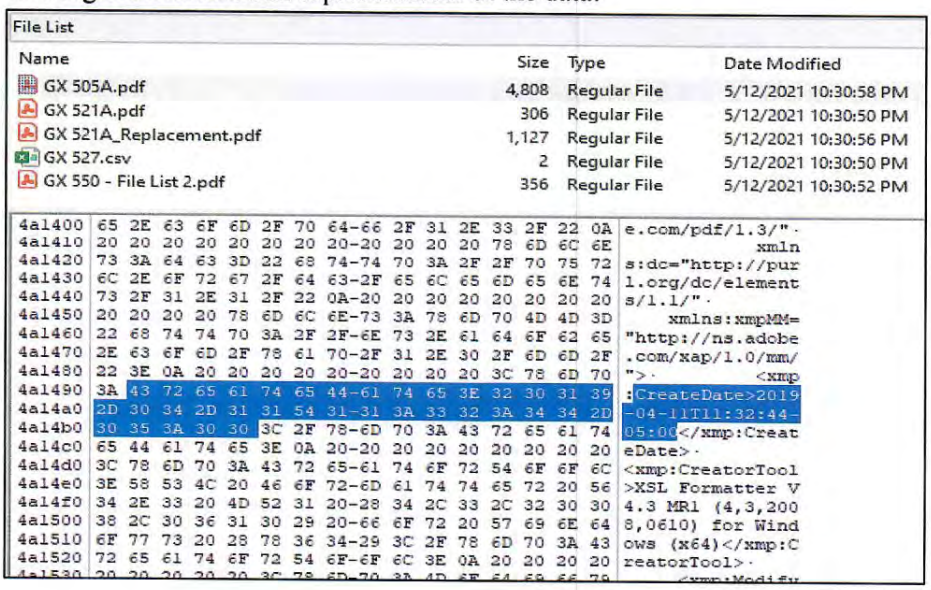
[3] See my Summary of Process Findings report for further details, found at *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.
[4] See my Summary of Technical Findings, Finding's #1 and #2, found at *Id.*
[5] For full disclosure, I am acquainted with SFE Flatley personally and have co-instructed 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.

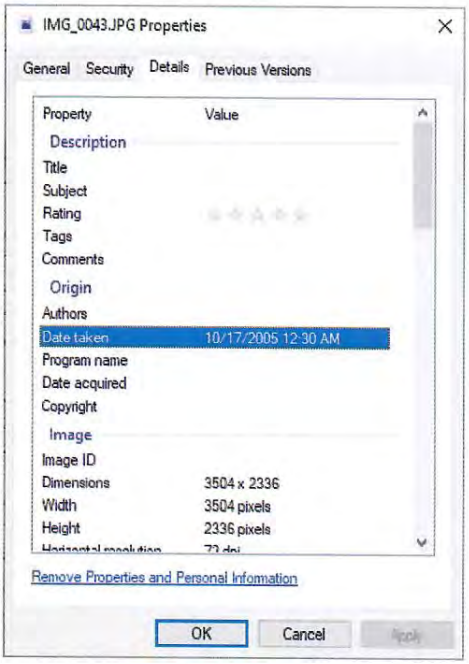


Using a forensic tool, FTK Imager, I verified that the date is indeed part of the *content* of the file, rather than stored elsewhere in the file system, by opening the same GX 505A.pdf document and viewing the hexadecimal representation of the data:



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.

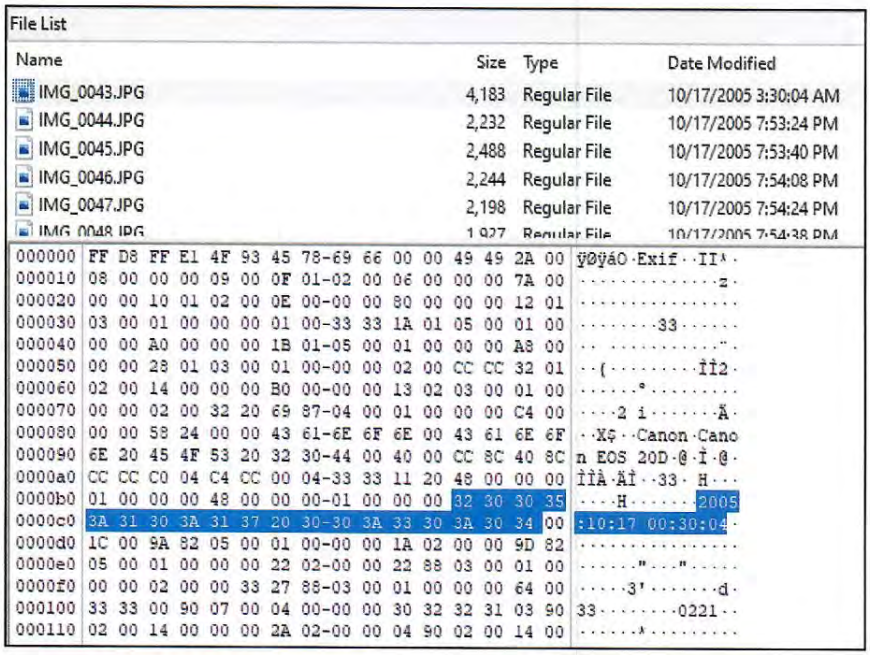
As SFE Flatley mentioned during his testimony, JPEG photo files also contains metadata, stored essentially in the same way, inside the content of the file as EXIF data. In the following screen shot I viewed the properties of "IMG_0043.JPG," a JPEG photo file in this case. The EXIF create date is displayed 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	1,927	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  ÿØÿáO·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  ··(·····ÌÌ2·
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  ··X$··Canon·Cano
000090 6E 20 45 4F 53 20 32 30-44 00 40 00 CC 8C 40 8C  n EOS 20D·@·Ì·@·
0000a0 CC CC C0 04 C4 CC 00 04-33 33 11 20 48 00 00 00  ÌÌÀ·ÄÌ··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 that[10]

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 files[11], 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 picture[12]

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 reliably of EXIF metadata[13]. 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] *Raniere, 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] *Raniere, 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 dates[23], 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.

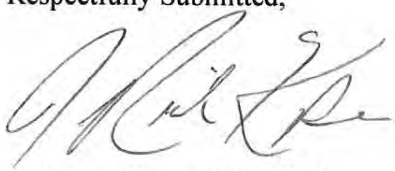
Consider SFE Flatley's expert opinions made under oath:

- 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."