Appendix A

A White Paper: EXIF Data and the Case "U.S. vs KEITH RANIERE"

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

Introduction

The purpose of this article is to expose the government's mischaracterization of EXIF data used as evidence against the defendant Keith Raniere.

Background

In this case, the prosecution claimed that Raniere used a Canon digital camera to take explicit photographs of a female while she was still a minor, saved them to a compact flash (CF) camera card, transferred them to an unknown computer, and then backed up those photographs to an external hard drive (See Figure 1).

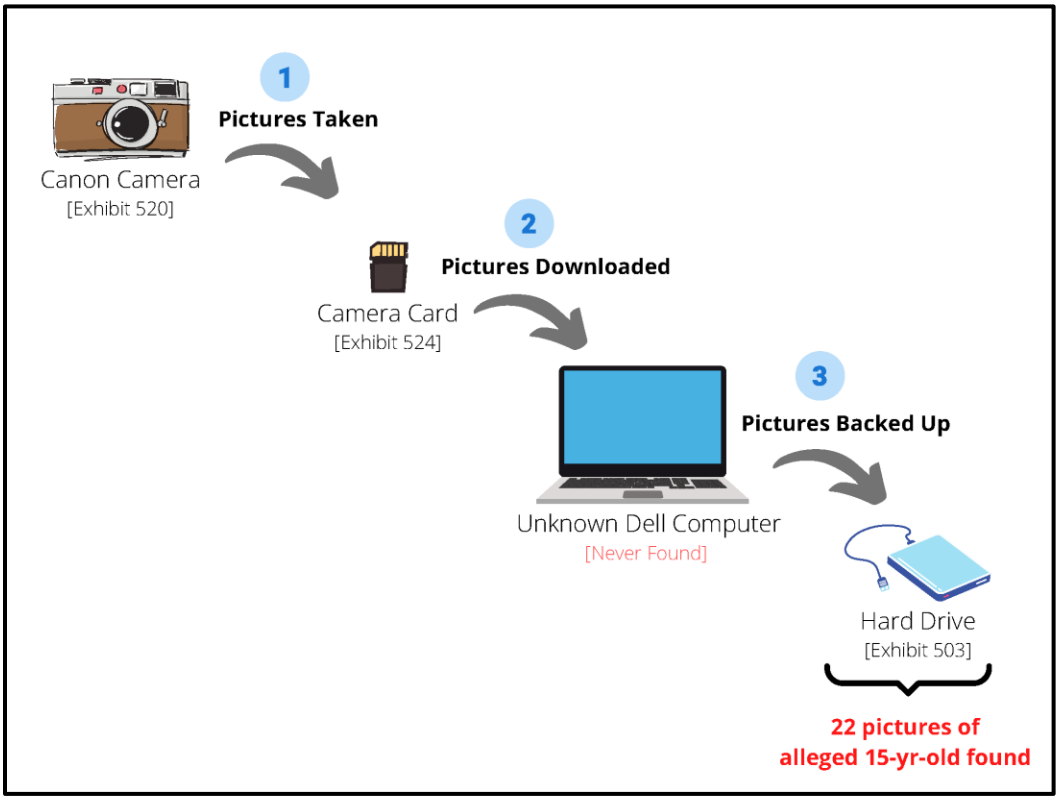

Figure 1: The Government's narrative regarding alleged contraband found on a "backup" drive.

To demonstrate that the alleged user of the camera, Raniere, created the alleged contraband, the prosecution needed to prove two things:

1. The alleged contraband photographs were taken in 2005, and
2. The alleged contraband photographs were taken with the camera allegedly used by Raniere.

The prosecution relied upon information embedded inside the digital photographs, called **Exchangeable Image Format (EXIF) data**, which records how the photo was taken, on what date, and with which camera settings. Since EXIF data is saved into to the *content* portion of the digital photograph file, it does not change when the photograph is transferred to another device.

The prosecution used the photo's EXIF data, specifically their creation date, to argue the subject was underage in the pictures. They also pointed to the fact that the EXIF data of the photos showed the same make and model of the camera allegedly used by Raniere. At first glance, this is a seemingly logical line of argumentation.

But one important question needs to be asked.

How reliable is EXIF data?

According to the FBI's expert witness, Senior Forensic Examiner William Booth, the photo EXIF data – the information that's embedded into the photograph file itself – is extremely reliable because it is "very hard" to change. Consider just a few of his statements from his court testimony (emphasis added):

Question: Is there a particular reason why **EXIF** data is **more difficult** to alter?
Booth: They purposely designed it that way.
Question: Do you know --
Booth: 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 (p.4820).

Booth: 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 (p.4830).

Booth: …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. (p.4977)

These are just a few of Booth's statements about the reliability of EXIF data and how hard it is to modify. Prosecutor Mark Lesko emphasized Booth's testimony in 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 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… (p.5572).

So both the FBI's expert witness and the DOJ prosecutor told the jury they could rely on the photo EXIF data to determine that Raniere had created the alleged contraband with the Canon camera in 2005 because the EXIF data is "extremely reliable" and "very hard" to modify.

However, is it true that digital photograph EXIF data is "very hard" to change? A simple demonstration will help answer this question.

Modifying Photograph EXIF Data

A quick Google search will enable anyone to find many of the freely-available, simple-to-use tools for editing EXIF data. One of my favorites is called **ExifTool**, which was recently featured in an online article titled, "7 Free Tools to Change Photo's Exif Data, Remove Metadata and Hide Dates" (https://www.geckoandfly.com/7987/how-to-change-exif-data-date-and-camera-properties-with-free-editor/). However – as I will demonstrate in a moment – a person doesn't even need to download a free tool to modify EXIF data.

For purposes of the following demonstration, I will use a real digital photograph from the U.S. vs KEITH RANIERE case. Although the photograph with the file name "IMG_0043.JPG" is simply a picture of a tree, it was found on the evidence "backup" hard drive along with the alleged contraband and it was allegedly taken with the same camera at around the same time. In Figure 2 below, the Microsoft Windows details pane (invoked by selecting the "View" tab of any Windows folder) is interpreting some of the EXIF data of IMG_0043.JPG.

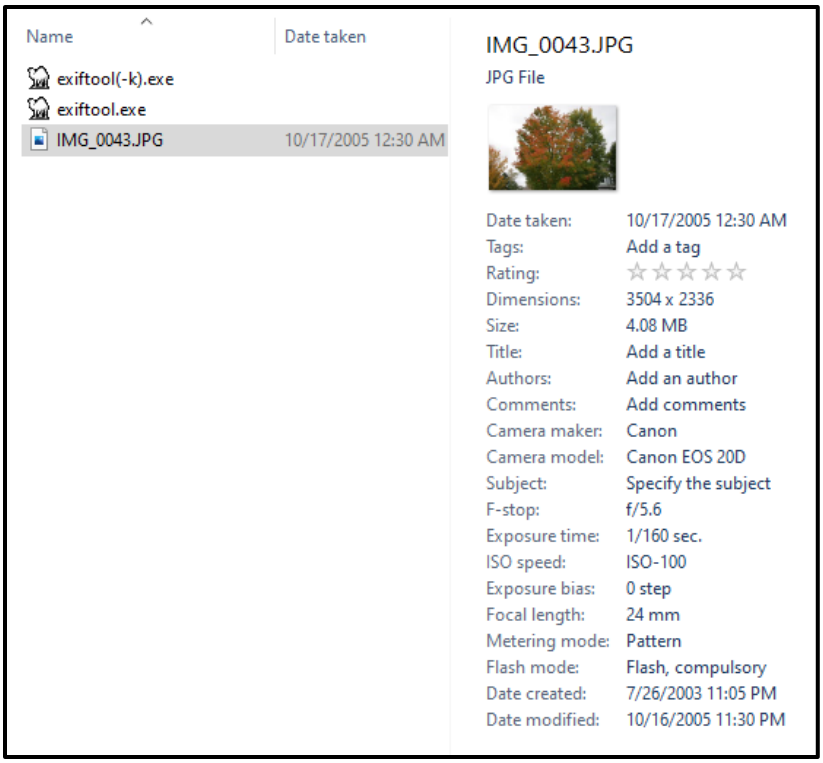

Figure 2. Windows display of EXIF data for IMG_0043.JPG.

According to the Windows display of EXIF data, this photo was taken on **10/17/2005** with a **Canon EOS 20D** digital camera. I verified this information by using the industry standard ExifTool I mentioned earlier. Here is how ExifTool interprets the EXIF data:

Figure 3. ExifTool display of EXIF data for IMG_0043.JPG.

How hard is it to change the camera model? In the Windows folder with the Details Pane enabled, I simply click the "Camera model" field and type whatever I want. Here I changed the camera model to an iPhone XR.

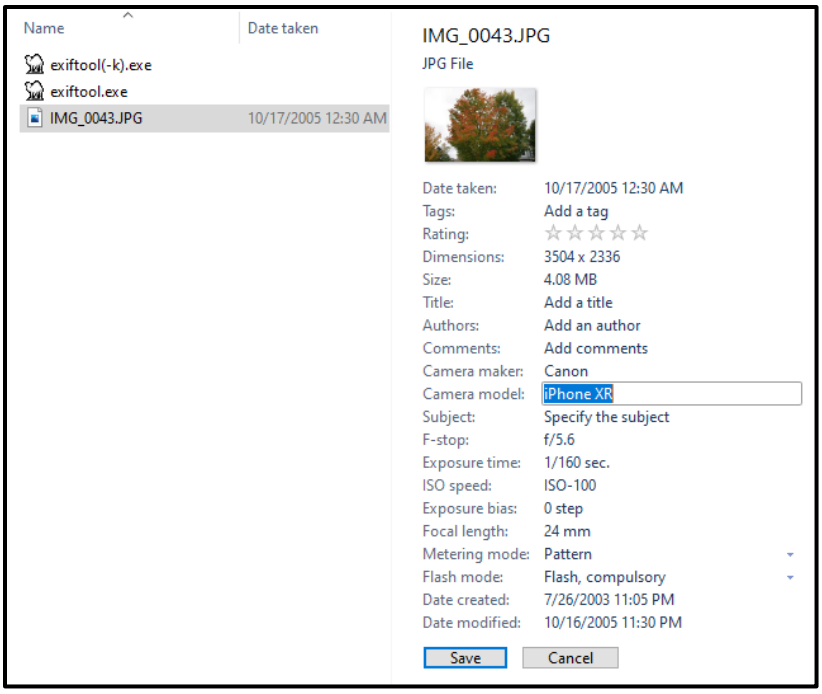

Figure 4. Changing the "Camera model" field in the EXIF data of a photo.

In the same way, I changed the Camera maker to Apple, and then I clicked on the "Date taken" field and set it to the United States Independence Day.

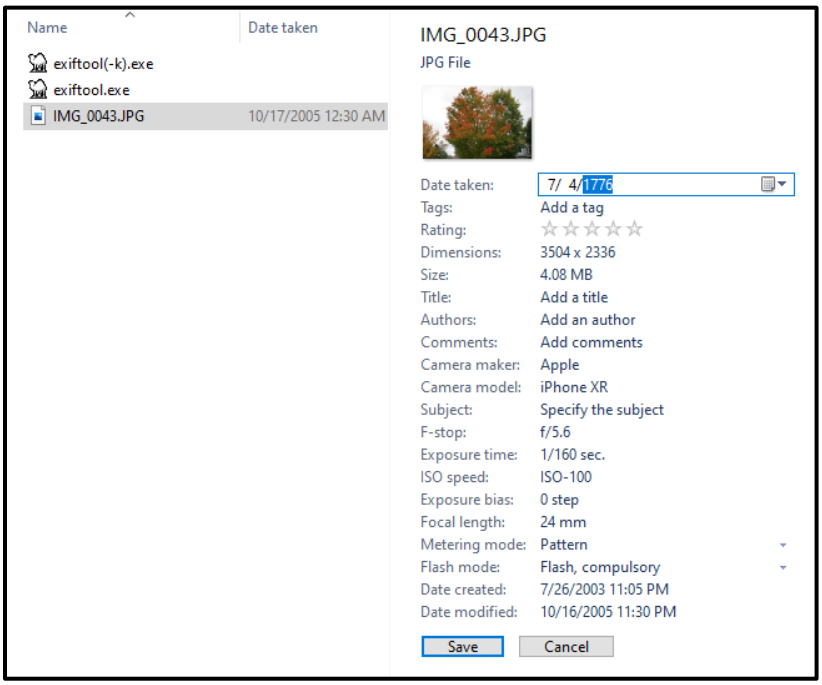

Figure 5. Changing the "Date taken" field in the EXIF data of a photo.

Therefore, a person viewing the file in Windows would now see a photo that was taken by an Apple iPhone XR, in the year 1776.

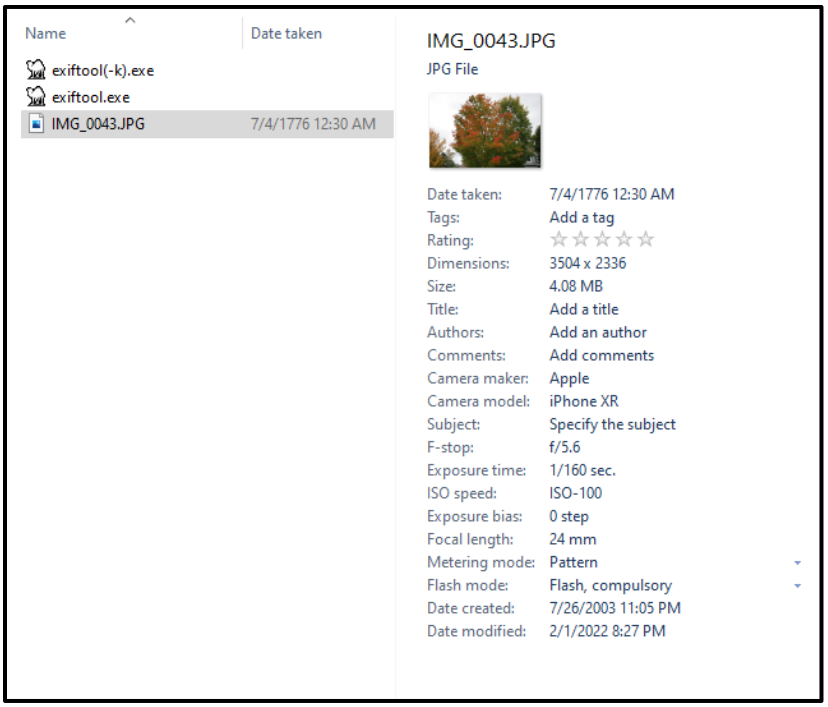

Figure 6. Windows display of saved changes in the EXIF data of photo IMG_0043.JPG.

Despite the government's contention in court, the EXIF data was very easy to change.

At this point a person might be thinking, "That's fine for the Windows interpretation, but was the EXIF data really modified?" To verify that the changes I made *in the Windows folder* in fact changed the EXIF data *in the file*, I opened the file again in ExifTool:

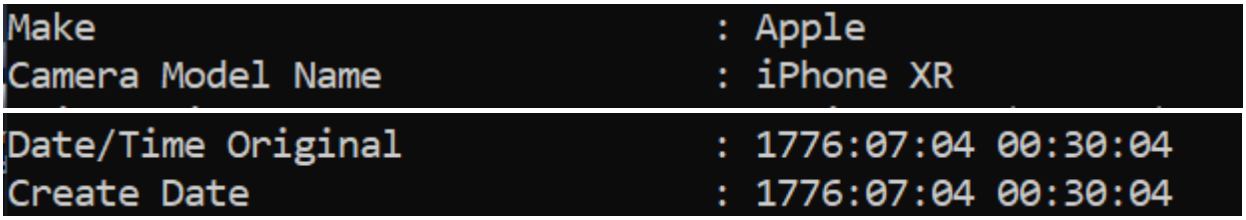

Figure 7. ExifTool display of saved changes in the EXIF data of photo IMG_0043.JPG.

The next question one might ask is: "What about a forensic tool? Would a digital forensic tool verify these changes in the EXIF portion of the file?"

One could argue that ExifTool is indeed a forensic tool, although it is in the public domain. But to put to rest any doubts about what happened, I viewed the photo in one of the most common (and FBI-approved) digital forensic tools available: AccessData's **FTK Imager**. In Figure 8

below, I imported IMG_0043.JPG and used the Hex viewer to read the raw EXIF data. All the EXIF changes I made were readily visible, and there were no traces to indicate that I or anyone else had ever made those changes.

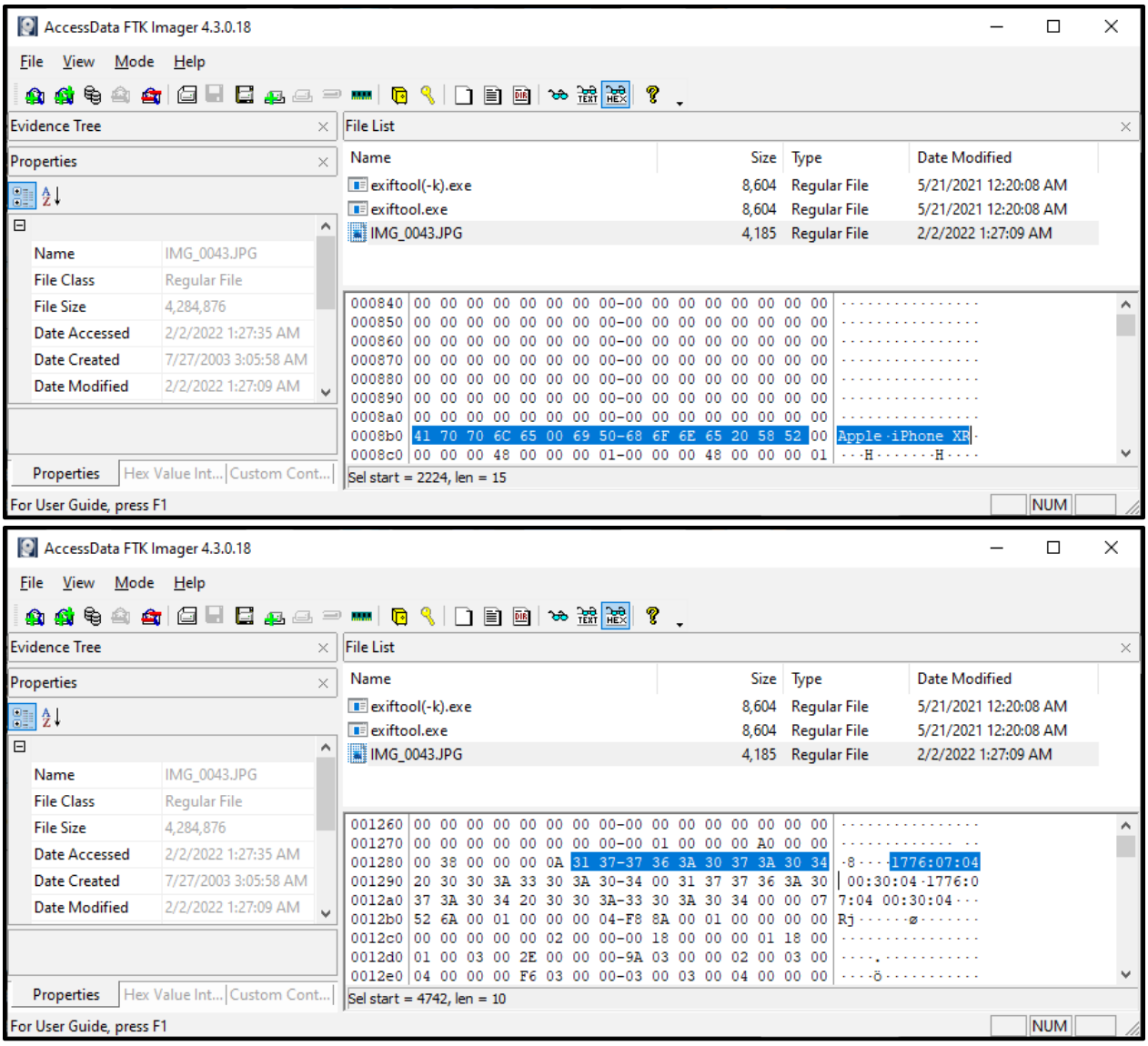

Figure 8. FTK Imager display of saved changes in the EXIF data of photo IMG_0043.JPG.

Conclusion

What does all this mean? <u>It means the government misled the jury about the nature of EXIF data used to convict Keith Raniere.</u>

I could have used one of the many freely available tools to modify the EXIF data that the government claimed was "extremely reliable" and "very hard" to modify. Instead, I simply used the **built-in features of Windows** to modify the EXIF data of one of the actual digital

photographs produced by the government at trial, and then I verified those changes in three different ways. In reality, anyone can reproduce what I just demonstrated in this article, using any digital photograph. Modifying EXIF data requires none of the "software" or "special processes" claimed by FBI examiner Booth, nor is it "very hard" to modify, as he claimed in sworn testimony. It is not clear to me why a Senior Forensic Examiner of his caliber would have made those false statements under oath.

Implications

Why would the FBI's star witness, the digital forensic examiner, swear under oath that EXIF data cannot be easily modified? And why would he make such statements multiple times during his testimony? I just demonstrated how easy it is.

The prosecution needed the jury to believe that EXIF data could not be easily modified because it was the only piece of digital information that supported the narrative that the photos on the drive allegedly belonging to Raniere were of an underage subject. If the prosecution had told the truth – that EXIF data can be easily modified with no special skills or tools – then the jury may have reasonably doubted its reliability as evidence of a crime.

The bottom line: It is a miscarriage of justice for the prosecution (and the jury) to have relied upon the authenticity of EXIF data to prove creation dates and the origin of digital photographs. If the government could blatantly mislead a jury about something so easy to disprove, it leaves me to ponder: What else were they lying about?

Respectfully submitted,

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