# 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 reports, 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:

- Summary of Technical Findings
- Summary of Process Findings
- Analysis of the Testimony of Special Agent Christopher Mills
- Expert Opinion Regarding Time to Review Digital Evidence

Signature: _____

Address: 818 Shannon Street
Tallahassee, Florida 32305

SUBSCRIBED AND SWORN TO before me this 25 day of April, 2022, by James Kiper.

_____
NOTARY PUBLIC FOR FLORIDA

Michael Jordan
Comm. # GG366579
Expires: October 1, 2023
Bonded Thru Aaron Notary

My Commission Expires: 10/1/23

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

# Summary of Technical Findings

## 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 (See attached CV). 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 an in-depth knowledge of FBI digital evidence examination procedures and policies.

## Review of Evidence

On May 21, 2021, I signed the Protective Order Regarding Discovery in U.S. v. Raniere, et al., 18 CR 204 (NGG) and was subsequently provided access to certain evidence in this case. My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports generated by members of the FBI's Computer Analysis Response Team (CART). Based on my review, I discovered specific actions that were taken to manually alter the evidence, in support of the government's narrative that photos were taken by a Canon EOS 20D camera (GX 520), saved to a Lexar CF card (GX 524), copied to an unknown computer, and then backed up to a Western Digital hard disk drive (GX 503). In this report I will refer to the latter two items as the CF Card and the WD HDD.

In my 20 years serving as an FBI agent, I have never observed or claimed that an FBI employee tampered with evidence, digital or otherwise. But in this case, I strongly believe the multiple, intentional alterations to the digital information I have discovered constitute evidence manipulation. And when so many human-generated alterations happen to align with the government's narrative, I believe any reasonable person would conclude that evidence tampering had taken place. My analysis demonstrates that some of these alterations definitely took place while the devices were in the custody of the FBI. Therefore, in the absence of any other plausible explanation it is my expert opinion that the FBI must have been involved in this evidence tampering.

**Key Findings**

1. Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.
2. Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.
3. An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.
4. Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.
5. The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.
6. The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.
7. The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

**Finding 1: Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.**

- As further explained in Finding #2, photos named IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG and IMG_0097.JPG (hereinafter IMG_0093-97) were among those that appeared on the FBI's WD HDD forensic report, but they did not initially appear on the CF Card forensic report generated on 04/11/2019. Subsequently, however, on 06/11/2019 the FBI created another version of the CF Card forensic report wherein these and other photo files were included. It is important to note that neither the IMG_0093-97 files, nor any other of the newly-added files, were **viewable** as photo images in the 06/11/2019 forensic report of the CF Card.
- The government's narrative requires that the IMG_0093-97 files on the second CF Card report be identical to the IMG_0093-97 files found in the WD HDD report, because photos created

on the CF Card were supposedly backed up to the WD HDD unaltered. Indeed, they have identical file names, identical Modified dates, and (presumably) identical EXIF data, including the date taken, camera model, and serial number[1]. However, they cannot be identical photo files because their MD5 hashes (**"digital fingerprints"**) do not match (See **Appendix A**, Figure 3).

- Moreover, a content review of the files reveals the subjects of the photographs found on the two devices are actually two different people. Although the IMG_0093-97 files were not viewable as photos in the 06/11/2019 CF Card report, their forensically recovered carved thumbnail photos were viewable, and they depicted a **blonde** woman. By contrast, the IMG_0093-97 files on the WD HDD report were viewable photographs and they depicted a **brunette** woman. Again, the two sets of IMG_0093-97 files share the same file names and the same last Modified dates and times – to the second. *This would mean the same camera, with the same serial number, took two different photographs of two different subjects at precisely the same time and assigned them the same file name.* This is impossible, of course, so the presence of these files indicates the manipulation of the content and metadata for these photos.
- In fact, a detailed analysis of the carved file listings for each device revealed that IMG_0093, IMG_0094, IMG_0096, and IMG_0097 found on the CF Card are not only different from their namesakes on the WD HDD, but they also **contain the same thumbnail images** as those of IMG_0180, IMG_0181, IMG_0182, and IMG_183, *respectively*. This surprising observation points to someone creating copies of IMG_0180–183 and then making changes to them on the CF card, including changing their file names to IMG_0093, IMG_0094, IMG_0096, and IMG_0097. These intentional alterations likely resulted in the files being unviewable on the 06/11/2019 forensic report, but it did not destroy the thumbnail images left over from the IMG_0180–0183 photos. It is likely the custodians of the CF Card who added these files, the case agents or their associates, repurposed the IMG_0180–183 files because at that time they did not have physical control of the WD HDD or its files. The FBI's Case Agent Investigative Review (CAIR) system enabled the case agents to review the WD HDD evidence and bookmark items, but it prevented them from exporting any information from the evidence. Please refer to **Appendix C** for an in-depth analysis of the carved files found in the WD HDD and CF Card forensic (FTK) reports.
- The intentional modification of the IMG_0093-97 files on the CF Card report cannot be explained by normal use of the camera or CF Card. In the context of this case, the alterations are best explained by the intentions of an unknown actor attempting to create a stronger relationship between the CF Card photo files and the WD HDD that supposedly contained their backups. These actions will be further explained in Finding 2.

[1] As noted in my Process Findings, neither the two forensic images of the CF card, nor the EXIF data from files in the associated FTK reports, were produced during discovery. However, I was able to determine that photographic data from IMG_0180 to IMG_0183, were actually found in the newly-added photos on the CF report with file names IMG_0093, IMG_0094, IMG_0096, and IMG_0097 (See **Appendix C**). If I had full access to the CF card data, it is reasonable to assume I would find the same EXIF data in those files as well.

**Finding 2: Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.**

- On 4/11/19, FBI forensic examiner Stephen Flatley created a forensic copy of the CF card, processed the data, and generated a forensic report using AccessData Forensic Toolkit (FTK), also known as AD LAB. The report listed active files present on the CF card, as well as those that had been deleted.
- On 6/11/19, five weeks into the trial and one day before he took the stand, FBI Examiner Brian Booth created *another* forensic copy and *another* FTK report of the same CF card. In the FBI, this is considered a reexamination and is prohibited by policy (see my Process Findings report). However, in this second report there were **new files** present in the file listing that **were not on the previous report**: Namely, IMG_0042, IMG_0081–IMG_0100, IMG_0172–IMG_0179, and IMG_0193–IMG_200.
- In the FBI, CART examiners generate FTK reports, which contain file listings, graphics, and exported files that were identified and bookmarked by the case agent or CART examiner. At times, new reports are generated from *existing forensic copies* of the same device, when the facts of the investigation change or when a new forensic tool becomes available. In this case, however, the difference between the two FTK reports cannot be attributed to the use of a different tool, because both examiners used the same tool and version number: AccessData Forensic Toolkit, Version 6.3.1.26.
- The appearance of new files on a subsequent forensic report does not, by itself, necessarily mean that files were added to the original device. However, I have generated hundreds of FTK reports for the FBI, and I can think of no legitimate reason for new files to appear on a subsequent FTK report generated by the same software and version number, working under the same set of facts, on the same piece of evidence, which is supposed to be preserved and immutable from the time of collection.
- In fact, there are several reasons to suspect that the new files appearing on the 06/11/2019 CF Card report did not legitimately originate on the CF Card itself:
    - None of the new files are viewable in the 06/11/2019 report, while all the files previously appearing on the 04/11/2019 report are viewable.
    - None of the new files are viewable on the CF Card report, so they cannot be visually compared with their namesakes on the WD HDD, which **are** viewable.
    - None of the **MD5 hashes** for the new files on the CF Card report match their namesakes on the WD HDD report. Mismatched MD5 hashes means they are not the same files.
    - Unlike the first 04/11 CF card report, the second 06/11 CF Card report **omitted the file sizes** for the photos, thereby preventing even a file size comparison of the new files with their namesakes on the WD HDD.
    - Aside from the manipulated IMG_0093-97 files discussed in Finding #1, the FBI's

forensic tool (FTK) was **unable to carve a single viewable photo** from any of the new files appearing on the 06/11 CF Card report. In that same report, by contrast, FTK was able to carve out several dozen **viewable photos from the CF Card's** previous photos as well as from unallocated space (with no links to specific files).

- To summarize, there is nothing besides easily-modifiable file names and file system dates and times that connect the new files in the 06/11 CF Card report with their namesake photos on the WD HDD report.

- Moreover, the way the new files appear on the 06/11/2019 CF Card report is indicative of someone creating large swaths **of "new files" on the CF Card ba**sed on file names, rather than on content. For example, as detailed in **Appendix D**, the appearance of 20 files (IMG_0081-100) on the second CF Card report implies that the user had taken several pictures of three different subjects, saved them to the CF Card and eventually backed them up to the WD HDD. However, it also requires the user to return to the CF Card, delete only first two photos (by filename) of the first subject, delete no photos of the second subject, and then delete all BUT the first two photos of the third subject. Even more incredibly, the user would have had to delete them in such a way as to prevent the FBI**'s forensic tool** (FTK) from recovering them (e.g. by writing over the sectors). As mentioned earlier, FTK had no problem recovering other deleted files, carving photos from those deleted files, or even recovering viewable photos from **the CF Card's** unallocated space.
- With the possible exception of IMG_0093-97 files discussed in Finding #1, the new files **appearing on the FBI's CF Card f**orensic report between the 04/11 and 06/11 versions **may not even be real digital photos**, since there is no data – no file sizes, no viewable images, no carved photos, no carved thumbnails – to indicate that they are. Nevertheless, these newly added CF card files and metadata match the filenames, dates, and times of files on the WD HDD, indicating that the likely reason for adding these files was to make it appear as though the corresponding files on the WD HDD at one time had originated on the CF card with the **dates indicated, consistent with the government's narrative. This is especially significant** because other than easily-modifiable EXIF data, there is no forensic evidence linking the hard **drive's alleged contraband to the CF card**. Again, for a detailed analysis of the new files appearing on the 06/11/2019 CF Card report, please see **Appendix D**.

**Finding 3: An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.**

- According to the CF card file listing (see **Appendix A**, Figure 1), the Accessed dates for *all the active files* were changed to 09/19/2018 (The rest of the files are recoverable deleted files). At a minimum, this finding demonstrates that file system dates on the CF card were altered on at least one occasion, 09/19/2018, six months after it was collected by the FBI on 03/27/2018.
- The presence of updated accessed dates also demonstrates the FBI did not use a write blocker **to preserve the evidence, which is a "critical procedure" according to FBI CART SOP 4.3** (see my Process Findings).

- According to the FBI Chain of Custody for the Camera and CF card, Case Agent Michael Lever checked out these items from Evidence Control on 09/19/2018 and returned them on 09/26/2018 (see **Appendix A**, Figure 2). SA Lever recorded his purpose for accepting custody as "Evidence Review." Therefore, SA Lever is most likely the person who accessed the CF card on 09/19/2018 without a write blocker. As I explain in my Process Findings report, this unauthorized access not only changed the evidence but it also violated FBI digital evidence handling policy.

**Finding 4: Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.**

- According to the file listing information in **Appendix B**, Table 1, there is an inconsistent relationship between two different dates presumably generated by the camera upon creation of the photographs. The EXIF date, generated by the camera, is embedded into the JPG file itself and does not change when the file is copied to another file system. However, the Modified date is saved to the CF card file system, and it may be interpreted differently by another computer, depending on that computer's time zone settings (The Created date is overwritten completely upon copy). I do not have access to the unknown computer into which the photographs were copied, so I have no information about its time zone settings. However, it appears a deliberate effort was made to alter Modified dates on the files so they might comport with the Daylight Saving Time, which ended 10/30/2005.
- From IMG_0043 to IMG_0126 the Modified dates were one hour behind those of the EXIF dates. On 10/30/2005 starting with IMG_0127 the Modified dates of photos were adjusted to be **two hours** behind, and then on the same day starting with IMG_0138 they were adjusted to be **exactly the same** as the EXIF dates. Notably, the photos IMG_0127-137 belong to a single folder (Mnp102005\2005-10-29-2350-08) and were the only photos on the WD HDD with this two-hour difference between the Modified dates and the EXIF dates. Nothing outside of human intervention could account for these changes.
- In my experience, there is likewise no legitimate reason a normal user would be making these changes.

**Finding 5: The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.**

- The Modified date of **IMG_0175** on the hard drive matches the Modified date of IMG_0175 recovered on the CF card, which would normally indicate that IMG_0175 was downloaded from the CF card onto an unknown computer and then copied to the hard drive without ever being modified.
- However, the EXIF CreatorTool value of IMG_0175 is set to "Adobe Photoshop Elements

3.0," which indicates that Adobe Photoshop was used to open and modify the file data. The Adobe Photoshop value could not have been set by the camera, and it was not observed in the EXIF data of any other photo. Since the EXIF data is part of the content portion of the file, its modification must result in an updated Modified date. The fact that the file's Modified dates are exactly the same on both devices - in the face of obvious modification - indicates the dates have been manually altered to be the same (See **Appendix A**, Figure 6).

- Modified dates are normally unaltered when copying to a new file system. Therefore, the act of altering a Modified date when content modification occurred reveals an intent by the user to conceal the file modification by coordinating the Modified dates between the CF card and the hard drive.
- The uniqueness of the EXIF data in the IMG_0175 file is also reflected in the thumbnail photo that was carved from it on the HDD. Every other carved thumbnail in this case is named "Carved [9728].jpeg," meaning it was carved at the end of the fixed length EXIF portion of the file located at byte offset 9728 (See **Appendix C** for a more detailed explanation). However, the thumbnail carved from IMG_0175 is named "Carved [9104].jpeg," meaning the EXIF data in this file is different from all the others.
- The fact that only one file, IMG_0175, still 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. Like the other files in the WD HDD, it contains the EXIF model and serial number of the camera, but none of the other files contains a reference to Photoshop.

**Finding 6: The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.**

- At trial the government acknowledged that the upper level folders, such as Df101905, were created by a human when FE Booth testified, "Yes, it looks like someone put the date and time associated with two letters" (p. 4984).
- However, during court proceedings the government repeatedly asked FE Booth to confirm both the upper level and lower level folder names (such as 2005-11-02-0422-20) "roughly" correspond to the original date and time contained in the EXIF data of files in those folders (e.g., pp. 4852-56). The clear implication was that these folder names could be relied upon to corroborate the values in the EXIF data. In fact, during closing arguments the government stated, "Brian Booth testified that the most reliable metadata that the FBI could obtain from the images on the Western digital hard drive, said that they were taken exactly when the folders stated they were taken" (p. 5371).
- The folders could not have been generated by the Canon camera, since that camera creates folders named "CANON100" to store the first 100 photos, "CANON200" for the second 100 photos, and so on. This folder naming convention appears in the file paths of both of the

government's FTK reports of the CF card, dated 04/11/2019 and 06/11/2019.

- Testing has demonstrated that Adobe Photoshop Elements can indeed create folder names with the YYYY-MM-DD-HHMM-SS nomenclature, but the date and time is based upon the current system clock at the time the photos were imported into Adobe Photoshop, not on the created times of the photos themselves. This fact reveals how the folder names were subsequently manipulated.
- According to the date/time nomenclature, for example, the folders "2005-10-19-0727-57" and "2005-10-19-0727-59" would have had to have been created two seconds apart (7:27:57 AM and 7:27:59 AM, respectively). These folders reside under separate and uniquely named parent folders, "Df101905" and "Msk101905," respectively (See **Appendix A**, Figure 5). The latter portion of these folder names could not possibly correspond to realistic folder creation times because two seconds is not enough time to manually select nine files, IMG_0090-98, copy them into the Df101905 folder, and then manually select another eleven files, IMG_0079-89, and manually navigate to the Msk101905 folder and save them there.
- In addition, I discovered a Thumbs.db file in each of the folders "2005-10-19-0727-57" and "2005-10-19-0727-59." In earlier versions of Windows, a Thumbs.db was automatically generated in a folder to contain previews of each file in the folder. However, I discovered that the Thumbs.db file in each of the "2005-10-19-0727-57" and "2005-10-19-0727-59" folders contain previews of **the full range of photos IMG_0079-98**. This means that all of those photos used to reside in a single folder in the *past*, and some time later they were divided and placed into their *current* locations, which are: IMG_0090-98 into the / Df101905/2005-10-19-0727-57/ folder and IMG_0079-89 into the /Msk101905/2005-10-19-0727-59/ folder. The fact that all photo previews were contained in both Thumbs.db files likely indicates that an earlier folder, containing all IMG_0079-98 photos, was duplicated, the resulting folders were renamed and placed into the Df101905 and Msk101905 folders, and then unwanted photos from each folder were removed. No special skills are required to move files and rename folders in the way I just described, and people often do so to organize photos according to subject matter.
- It is certain that some of the timestamped folder names were manually manipulated, such as the ones described above. Given the ease with which one can alter folder names, it is possible the names of the folders containing alleged contraband (2005-11-02-0422-20 and 2005-11-24-0814-46) were manually set in a way that aligns with the prosecution's narrative that the photos were taken in November 2005, and therefore the subject would have been fifteen years old, according to the trial record. At the very least, the dates and times indicated in these folder names cannot be relied upon to determine or corroborate the creation dates of the photos contained in them.

**Finding 7: The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates**.

- According to the file listing of a forensically imaged Western Digital hard drive (WD HDD), on 03/30/2009 a backup was made of a Dell Inspiron 700M and given the folder name "BKP.DellInspiron700M-20090330." Also on 03/30/2009 a PowerMac was backed up to the folder "BKP.PowerMac8.2-2009-0330." Unsurprisingly, all the Created dates in these folders were 03/30/2009 (or very early 03/31/2009), the backup date identified in the folder name (see **Appendix A**, Figure 4). By contrast, all the files in the unknown computer ("Dell Dimension") backup folder ("BKP.DellDimension8300-20090330") have a Created date of 07/26/2003, and the backup folder has a last Accessed date of 07/28/2003, despite the folder *name* indicating the same backup date as the others (03/30/2009).
- When files are copied from one file system to another, their Created dates are changed to the current clock time of the machine hosting the receiving file system. If all clocks are accurate, then the created time of these copied files will necessarily be AFTER the modified times.
- In this case, however, all the files in the unknown computer backup ("BKP.DellDimension8300-20090330") have a Created date of 07/26/2003, while most of their Modified dates are from October 2005 and later. This observation indicates the system clock was rolled back to 2003 before copying these files manually onto the hard drive.
- Sometimes the computer's CMOS battery – which enables the computer to retain information after shutdown such as system time – goes bad, resulting in the system clock being reset to a default date, such as 01/01/2003[2]. However, the computer will continue to reset the system clock to that date every time the computer powers up. Therefore, a bad CMOS battery cannot explain the system clock set to 07/26/2003 for the creation date of the files in the folder whose name, as mentioned previously, indicates a 03/30/2009 backup. It also fails to explain the creation dates of several hundred (mostly music) files copied to the WD HDD between 08/08/2003 and 08/18/2003 that were NOT located in the "BACKUPS" folder.
- The rolling back of the system clock is more likely the result of someone who was trying to backdate the folder content and make this folder appear to be a legitimate backup folder but may not have considered how and when file system dates are normally updated.

There are other significant anomalies in this backup folder that showcase the failed effort to create the appearance of an automated backup:

- The Dell Inspiron backup contains more than 15,000 files, while Dell Dimension backup was backed up in two separate copy operations, in total less than 500 files.
- The Dell Inspiron backup included several directories, such as Desktop, Favorites, and My

[2] Although the "factory default" date could theoretically be any date, I have never seen one that is NOT on the first day of the month, either in January or December of the year of manufacture.

Documents, while the Dell Dimension backup initially only included the Studies folder, containing the images in question. It is uncommon for a user to choose to primarily back up a particular folder (in this case, the "Studies" folder) from an entire desktop system, while ignoring more common file storage locations such as My Documents. To accept the legitimacy of this backup one would need to believe a highly improbable scenario where the user made a concerted effort to back up a folder containing his contraband, and specifically this folder, from an entire desktop system. In a likely attempt to create the appearance of a legitimate backup – more than an hour after the "Studies" files were copied – a Symantec folder with one file, and about 150 songs were added to the backup folder.

**Conclusion**

In summary, the forensic evidence shows that folder names and dates (key facts upon which the prosecution's argument relied) were manually altered, and the entire backup folder to which the alleged contraband belonged was manipulated. While it is impossible to determine exactly when the information on the WD HDD was altered, it is a scientific certainty that data on the CF card were added and/or modified while the device was in FBI custody.

Respectfully Submitted,

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

## Appendix A: Figures

Figure 1. CF card file listing showing 9/19/2018 access dates[3].

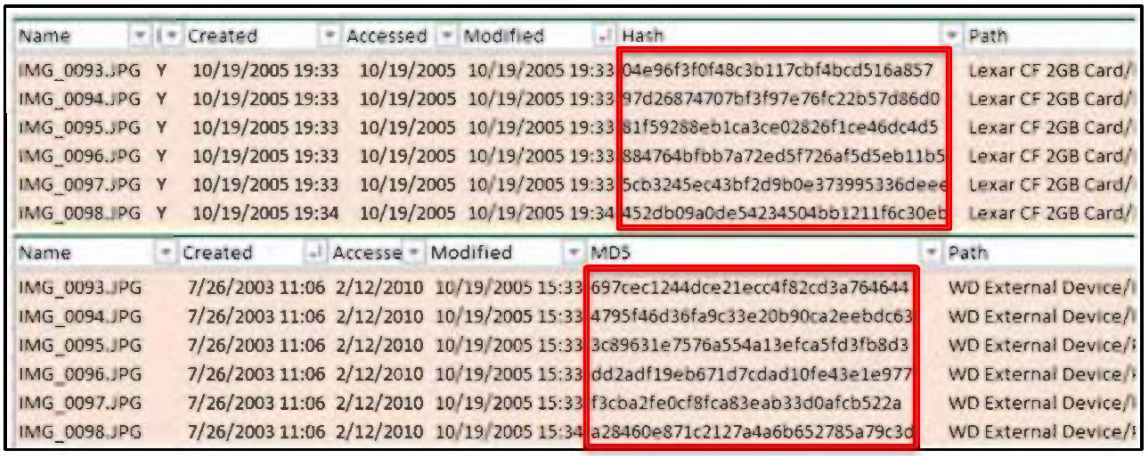
| Name | Delete | Created | Accessed | Modified | Hash | Path |
|---|---|---|---|---|---|---|
| IMG_0224.JPG | N | 3/9/2006 3:18 | 9/19/2018 | 3/9/2006 3:18 | 596a4251cf7782a440d9b6e8c5c18720 | Lexar CF 2GB Card/ |
| IMG_0225.JPG | N | 3/9/2006 3:18 | 9/19/2018 | 3/9/2006 3:18 | 1b613027ddb1bafcfcfa88ffd20c6f1e | Lexar CF 2GB Card/ |
| IMG_0227.JPG | N | 3/9/2006 3:19 | 9/19/2018 | 3/9/2006 3:19 | f7ac8c54897985961f729299756fc319 | Lexar CF 2GB Card/ |
| IMG_0228.JPG | N | 3/9/2006 3:19 | 9/19/2018 | 3/9/2006 3:19 | 341c44c7bd25375f6aeedf39a8db79cc | Lexar CF 2GB Card/ |
| IMG_0229.JPG | N | 3/9/2006 3:19 | 9/19/2018 | 3/9/2006 3:19 | b5ea586450d43d25eda07fffb7f76f82 | Lexar CF 2GB Card/ |
| IMG_0230.JPG | N | 3/9/2006 3:20 | 9/19/2018 | 3/9/2006 3:20 | 4836010357e1ba89baade965f3d89a0b | Lexar CF 2GB Card/ |
| IMG_0231.JPG | N | 3/9/2006 3:20 | 9/19/2018 | 3/9/2006 3:20 | 8bdce71ed54222d649badfcc2d75d898 | Lexar CF 2GB Card/ |
| IMG_0233.JPG | N | 3/9/2006 3:20 | 9/19/2018 | 3/9/2006 3:20 | 83962b67a98f299f67e6262317c601d5 | Lexar CF 2GB Card/ |
| IMG_0234.JPG | N | 3/9/2006 3:20 | 9/19/2018 | 3/9/2006 3:20 | 760ac0e77c1d9455c28c07836c52c32b | Lexar CF 2GB Card/ |
| IMG_0235.JPG | N | 3/9/2006 3:21 | 9/19/2018 | 3/9/2006 3:21 | d597dbff4c67fb186b55eff1862e330e | Lexar CF 2GB Card/ |
| IMG_0236.JPG | N | 3/9/2006 3:21 | 9/19/2018 | 3/9/2006 3:21 | 534518d5b7cb5e4ab864c04890642294 | Lexar CF 2GB Card/ |
| IMG_0237.JPG | N | 3/9/2006 3:22 | 9/19/2018 | 3/9/2006 3:22 | a280f9c541fa96731628987baec67095 | Lexar CF 2GB Card/ |
| IMG_0238.JPG | N | 3/9/2006 3:22 | 9/19/2018 | 3/9/2006 3:22 | 30788af5673e78bf0365dfb39776d4a9 | Lexar CF 2GB Card/ |
| IMG_0239.JPG | N | 3/9/2006 3:22 | 9/19/2018 | 3/9/2006 3:22 | de746ef94d03b6c01797914747cb3601 | Lexar CF 2GB Card/ |
| IMG_0241.JPG | N | 1/6/2007 7:03 | 9/19/2018 | 1/6/2007 7:03 | e306c5177fc9cd747dde978233674043 | Lexar CF 2GB Card/ |
| IMG_0242.JPG | Y | 1/6/2007 7:05 | 1/6/2007 | 1/6/2007 7:05 | ba9411b3b34b626f73ee4649c757654 | Lexar CF 2GB Card/ |
| IMG_0243.JPG | N | 1/6/2007 7:05 | 9/19/2018 | 1/6/2007 7:05 | 3b77bc0a1f64652b820d1804b88a8d80 | Lexar CF 2GB Card/ |

Figure 2. Excerpt from DX 945, Chain of Custody for Camera and CF Card, showing SA Lever checking out evidence on 09/19/2018 and returning it on 09/26/2018.

| Relinquished Custody | Date and Time | Accepted Custody | Date and Time |
|---|---|---|---|
| Signature: | 9/19/18 | Signature: | 9/19/18 |
| Printed Name/Agency: Corey Montgomery | 0900 | Printed Name/Agency: Michael Lever FBI | 0900 |
| Reason: C/O to SA | | Reason: Evidence Review | |
| **Relinquished Custody** | **Date and Time** | **Accepted Custody** | **Date and Time** |
| Signature: | 9/26/18 | Signature: | 9/26/18 |
| Printed Name/Agency: Michael Lever FBI | 1:15PM | Printed Name/Agency: | 1:15PM |
| Reason: Evidence Return | | Reason: | |

[3] **Note**: The HDD listing referenced in Figures 1, 3, 4, and 5 was generated by the defense using a computer set to Pacific Time while the government reports were generated by a computer set to Eastern Time.

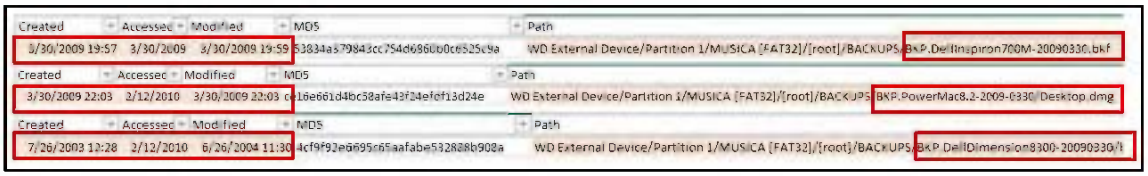
Figure 3. Comparison of photograph metadata for files found on both the CF card and WD HDD.



| Name | | Created | Accessed | Modified | Hash | Path |
|---|---|---|---|---|---|---|
| IMG_0093.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 04e96f3f0f48c3b117cbf4bcd516a857 | Lexar CF 2GB Card/ |
| IMG_0094.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 97d26874707bf3f97e76fc22b57d86d0 | Lexar CF 2GB Card/ |
| IMG_0095.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 81f59288eb1ca3ce02826f1ce46dc4d5 | Lexar CF 2GB Card/ |
| IMG_0096.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 884764bfbb7a72ed5f726af5d5eb11b5 | Lexar CF 2GB Card/ |
| IMG_0097.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 5cb3245ec43bf2d9b0e373995336deee | Lexar CF 2GB Card/ |
| IMG_0098.JPG | Y | 10/19/2005 19:34 | 10/19/2005 | 10/19/2005 19:34 | 452db09a0de54234504bb1211f6c30eb | Lexar CF 2GB Card/ |

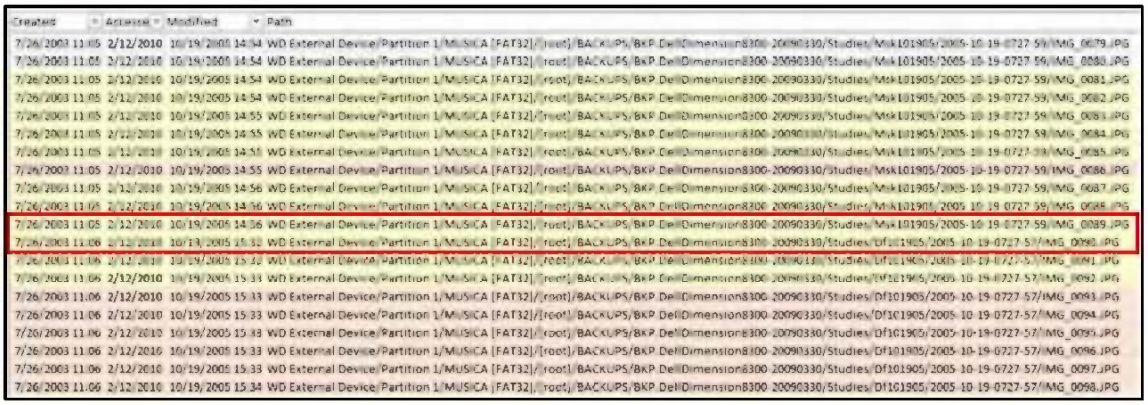
| Name | Created | Accesse | Modified | MD5 | Path |
|---|---|---|---|---|---|
| IMG_0093.JPG | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | 697cec1244dce21ecc4f82cd3a764644 | WD External Device/I |
| IMG_0094.JPG | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | 4795f46d36fa9c33e20b90ca2eebdc63 | WD External Device/I |
| IMG_0095.JPG | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | 3c89631e7576a554a13efca5fd3fb8d3 | WD External Device/I |
| IMG_0096.JPG | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | dd2adf19eb671d7cdad10fe43e1e977 | WD External Device/I |
| IMG_0097.JPG | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | f3cba2fe0cf8fca83eab33d0afcb522a | WD External Device/I |
| IMG_0098.JPG | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:34 | a28460e871c2127a4a6b652785a79c3c | WD External Device/I |

Figure 4. Records from the WD HDD File listing showing disparity in Created dates.



| Created | Accessed | Modified | MD5 | Path |
|---|---|---|---|---|
| 3/30/2009 19:57 | 3/30/2009 | 3/30/2009 19:59 | 53834a579843cc754d6860b0c6525c9a | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellInspiron700M-20090330.bkf |
| Created | Accessed | Modified | MD5 | Path |
| 3/30/2009 22:03 | 2/12/2010 | 3/30/2009 22:03 | c16e661d4bc58afe43f24efcf13d24e | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.PowerMac8.2-2009-0330/Desktop.dmg |
| Created | Accessed | Modified | MD5 | Path |
| 7/26/2003 12:28 | 2/12/2010 | 6/26/2004 11:30 | 4cf9f92e6695c65aafabe532828b908a | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/I |

Figure 5. The WD HDD file listing showing the disparity of parent folders and date/time stamps.



| Created | Accessed | Modified | Path |
|---|---|---|---|
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:54 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0079.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:54 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0080.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:54 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0081.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:54 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0082.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:55 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0083.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:55 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0084.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:55 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0085.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:55 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0086.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:56 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0087.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:56 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0088.JPG |
| 7/26/2003 11:05 | 2/12/2010 | 10/19/2005 14:56 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727 59/IMG_0089.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:32 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0090.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:32 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0091.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0092.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0093.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0094.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0095.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0096.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0097.JPG |
| 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:34 | WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727 57/IMG_0098.JPG |

Figure 6. A comparison of Modified Dates for IMG_0175.JPG, which was modified.

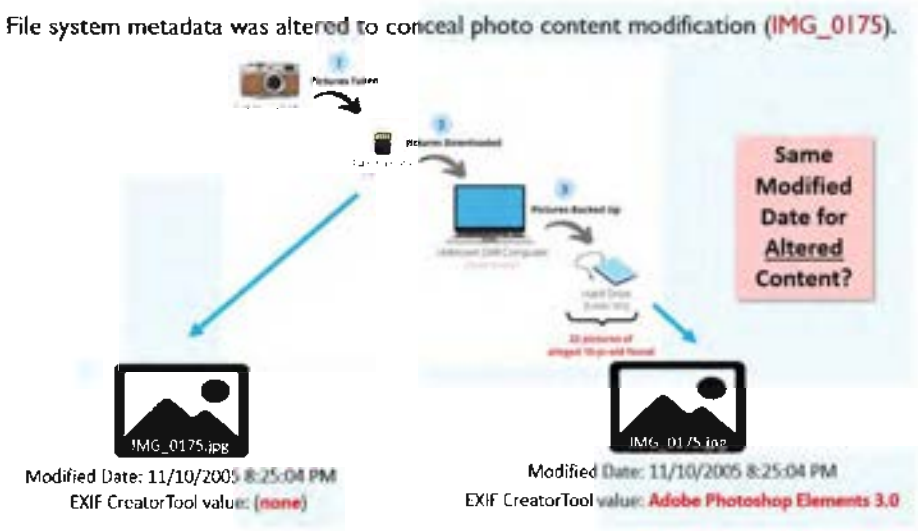
Figure 6a. IMG_0175 file system metadata from the recovered deleted file on the **CF Card** (GX 521 Replacement). This copy could NOT have contained an EXIF CreatorTool value set to **"Photoshop Adobe Elements 3.0".**

**Name** IMG_0175.JPG
**Extension** jpg
**Item Number** 1064
**Path** Lexar CF 2GB Card/Partition 1/LEXAR MEDIA |FAT16|/|root|/DCIM/101CANON/I
MG_0175.JPG
**Created Date** 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
**Accessed Date** 11/10/2005
**Modified Date** 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
**MD5 Hash**
**Deleted** True
**Carved** False

Figure 6b. IMG_0175 file system metadata from the **HDD** (GX 505A). This copy contained **EXIF data with a CreatorTool value set to "Photoshop Adobe Elements 3.0".**

**Name** IMG_0175.JPG
**Created Date** 7/26/2003 2:06:31 PM (2003-07-26 18:06:31 UTC)
**Accessed Date** 2/12/2010
**Modified Date** 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
**MD5 Hash** 44725d873418dbff665de0198463f20c9
**Path** 1B16 WD HD 500GB/Partition 1/MUSICA |FAT32|/|root|/BACKUPS/
BKP.DellDimension8300-20090330/Studies/A111005/2005-11-10-0718-42/IMG_0175.JPG
**Exported as** Report_Files/files/IMG_0175.JPG

Figure 6c. File system metadata was altered to conceal EXIF data modification and support the **government's narrative.**



## Appendix B: File Listing Tables

### Table 1: Pictures on hard drive under "Studies" on the hard drive (GX 503)

| File Name | WD HDD FAT Modified Date | WD HDD EXIF DateTimeOriginal | Time Shift Between FAT Modified and EXIF DateTimeOriginal (within a few seconds) |
|---|---|---|---|
| IMG_0043.JPG | 10/16/05 11:30:04 PM | 10/17/05 12:30:04 AM | 1 |
| IMG_0044.JPG | 10/17/05 3:53:24 PM | 10/17/05 4:53:22 PM | 1 |
| IMG_0045.JPG | 10/17/05 3:53:40 PM | 10/17/05 4:53:40 PM | 1 |
| IMG_0046.JPG | 10/17/05 3:54:08 PM | 10/17/05 4:54:09 PM | 1 |
| IMG_0047.JPG | 10/17/05 3:54:24 PM | 10/17/05 4:54:24 PM | 1 |
| IMG_0048.JPG | 10/17/05 3:54:38 PM | 10/17/05 4:54:38 PM | 1 |
| IMG_0049.JPG | 10/17/05 3:54:54 PM | 10/17/05 4:54:54 PM | 1 |
| IMG_0050.JPG | 10/17/05 3:55:04 PM | 10/17/05 4:55:05 PM | 1 |
| IMG_0051.JPG | 10/17/05 3:55:28 PM | 10/17/05 4:55:28 PM | 1 |
| IMG_0052.JPG | 10/17/05 3:55:42 PM | 10/17/05 4:55:41 PM | 1 |
| IMG_0053.JPG | 10/17/05 3:55:54 PM | 10/17/05 4:55:52 PM | 1 |
| IMG_0054.JPG | 10/17/05 3:55:58 PM | 10/17/05 4:55:59 PM | 1 |
| IMG_0055.JPG | 10/17/05 3:56:24 PM | 10/17/05 4:56:25 PM | 1 |
| IMG_0056.JPG | 10/17/05 3:56:36 PM | 10/17/05 4:56:36 PM | 1 |
| IMG_0057.JPG | 10/17/05 3:56:48 PM | 10/17/05 4:56:48 PM | 1 |
| IMG_0058.JPG | 10/17/05 3:56:58 PM | 10/17/05 4:56:58 PM | 1 |
| IMG_0059-1.JPG | 10/17/05 9:00:58 PM | 10/17/05 10:00:57 PM | 1 |
| IMG_0060-1.JPG | 10/17/05 9:01:06 PM | 10/17/05 10:01:07 PM | 1 |
| IMG_0061-1.JPG | 10/17/05 9:01:12 PM | 10/17/05 10:01:13 PM | 1 |
| IMG_0062-1.JPG | 10/17/05 9:01:24 PM | 10/17/05 10:01:24 PM | 1 |
| IMG_0063-1.JPG | 10/17/05 9:01:32 PM | 10/17/05 10:01:32 PM | 1 |
| IMG_0064-1.JPG | 10/17/05 9:02:00 PM | 10/17/05 10:02:00 PM | 1 |

| | | | |
|---|---|---|---|
| IMG_0065-1.JPG | 10/17/05 9:02:08 PM | 10/17/05 10:02:07 PM | 1 |
| IMG_0066-1.JPG | 10/17/05 9:02:14 PM | 10/17/05 10:02:13 PM | 1 |
| IMG_0067-1.JPG | 10/17/05 9:02:34 PM | 10/17/05 10:02:34 PM | 1 |
| IMG_0068-1.JPG | 10/17/05 9:03:02 PM | 10/17/05 10:03:01 PM | 1 |
| IMG_0069-1.JPG | 10/17/05 9:03:10 PM | 10/17/05 10:03:10 PM | 1 |
| IMG_0070-1.JPG | 10/17/05 9:03:24 PM | 10/17/05 10:03:24 PM | 1 |
| IMG_0071.JPG | 10/18/05 7:32:06 PM | 10/18/05 8:32:06 PM | 1 |
| IMG_0072.JPG | 10/18/05 7:32:26 PM | 10/18/05 8:32:26 PM | 1 |
| IMG_0073.JPG | 10/18/05 7:32:36 PM | 10/18/05 8:32:36 PM | 1 |
| IMG_0074.JPG | 10/18/05 7:32:44 PM | 10/18/05 8:32:44 PM | 1 |
| IMG_0075.JPG | 10/18/05 7:33:08 PM | 10/18/05 8:33:09 PM | 1 |
| IMG_0076.JPG | 10/18/05 7:33:14 PM | 10/18/05 8:33:15 PM | 1 |
| IMG_0077.JPG | 10/18/05 7:33:22 PM | 10/18/05 8:33:22 PM | 1 |
| IMG_0078.JPG | 10/18/05 7:33:30 PM | 10/18/05 8:33:30 PM | 1 |
| IMG_0079.JPG | 10/19/05 5:54:08 PM | 10/19/05 6:54:09 PM | 1 |
| IMG_0080.JPG | 10/19/05 5:54:22 PM | 10/19/05 6:54:23 PM | 1 |
| IMG_0081.JPG | 10/19/05 5:54:32 PM | 10/19/05 6:54:33 PM | 1 |
| IMG_0082.JPG | 10/19/05 5:54:56 PM | 10/19/05 6:54:57 PM | 1 |
| IMG_0083.JPG | 10/19/05 5:55:10 PM | 10/19/05 6:55:10 PM | 1 |
| IMG_0084.JPG | 10/19/05 5:55:36 PM | 10/19/05 6:55:37 PM | 1 |
| IMG_0085.JPG | 10/19/05 5:55:48 PM | 10/19/05 6:55:49 PM | 1 |
| IMG_0086.JPG | 10/19/05 5:55:56 PM | 10/19/05 6:55:57 PM | 1 |
| IMG_0087.JPG | 10/19/05 5:56:08 PM | 10/19/05 6:56:09 PM | 1 |
| IMG_0088.JPG | 10/19/05 5:56:24 PM | 10/19/05 6:56:24 PM | 1 |
| IMG_0089.JPG | 10/19/05 5:56:34 PM | 10/19/05 6:56:34 PM | 1 |
| IMG_0090.JPG | 10/19/05 6:32:52 PM | 10/19/05 7:32:51 PM | 1 |
| IMG_0091.JPG | 10/19/05 6:32:58 PM | 10/19/05 7:32:57 PM | 1 |

| | | | |
|---|---|---|---|
| IMG_0092.JPG | 10/19/05 6:33:08 PM | 10/19/05 7:33:09 PM | 1 |
| IMG_0093.JPG | 10/19/05 6:33:18 PM | 10/19/05 7:33:18 PM | 1 |
| IMG_0094.JPG | 10/19/05 6:33:26 PM | 10/19/05 7:33:25 PM | 1 |
| IMG_0095.JPG | 10/19/05 6:33:30 PM | 10/19/05 7:33:29 PM | 1 |
| IMG_0096.JPG | 10/19/05 6:33:52 PM | 10/19/05 7:33:51 PM | 1 |
| IMG_0097.JPG | 10/19/05 6:33:58 PM | 10/19/05 7:33:57 PM | 1 |
| IMG_0098.JPG | 10/19/05 6:34:08 PM | 10/19/05 7:34:08 PM | 1 |
| IMG_0099.JPG | 10/20/05 3:20:12 PM | 10/20/05 4:20:13 PM | 1 |
| IMG_0100.JPG | 10/20/05 3:20:30 PM | 10/20/05 4:20:31 PM | 1 |
| IMG_0101.JPG | 10/20/05 3:20:44 PM | 10/20/05 4:20:44 PM | 1 |
| IMG_0102.JPG | 10/20/05 3:21:02 PM | 10/20/05 4:21:02 PM | 1 |
| IMG_0103.JPG | 10/20/05 3:21:28 PM | 10/20/05 4:21:28 PM | 1 |
| IMG_0104.JPG | 10/20/05 3:25:14 PM | 10/20/05 4:25:14 PM | 1 |
| IMG_0105.JPG | 10/20/05 3:26:56 PM | 10/20/05 4:26:56 PM | 1 |
| IMG_0106.JPG | 10/20/05 3:27:04 PM | 10/20/05 4:27:03 PM | 1 |
| IMG_0107.JPG | 10/20/05 3:49:24 PM | 10/20/05 4:49:23 PM | 1 |
| IMG_0108.JPG | 10/20/05 3:49:26 PM | 10/20/05 4:49:26 PM | 1 |
| IMG_0109.JPG | 10/20/05 3:49:30 PM | 10/20/05 4:49:29 PM | 1 |
| IMG_0110.JPG | 10/29/05 4:11:16 AM | 10/29/05 5:11:16 AM | 1 |
| IMG_0111.JPG | 10/29/05 4:11:42 AM | 10/29/05 5:11:43 AM | 1 |
| IMG_0112.JPG | 10/29/05 4:43:36 AM | 10/29/05 5:43:36 AM | 1 |
| IMG_0113.JPG | 10/29/05 4:43:54 AM | 10/29/05 5:43:54 AM | 1 |
| IMG_0115.JPG | 10/29/05 4:44:52 AM | 10/29/05 5:44:52 AM | 1 |
| IMG_0116.JPG | 10/29/05 4:44:56 AM | 10/29/05 5:44:55 AM | 1 |
| IMG_0117.JPG | 10/29/05 4:45:06 AM | 10/29/05 5:45:06 AM | 1 |
| IMG_0118.JPG | 10/29/05 4:45:20 AM | 10/29/05 5:45:20 AM | 1 |
| IMG_0119.JPG | 10/29/05 4:45:26 AM | 10/29/05 5:45:25 AM | 1 |

| | | | |
|---|---|---|---|
| IMG_0120.JPG | 10/29/05 4:45:40 AM | 10/29/05 5:45:40 AM | 1 |
| IMG_0121.JPG | 10/29/05 4:45:50 AM | 10/29/05 5:45:50 AM | 1 |
| IMG_0122.JPG | 10/29/05 4:46:00 AM | 10/29/05 5:46:00 AM | 1 |
| IMG_0123.JPG | 10/29/05 4:47:00 AM | 10/29/05 5:46:59 AM | 1 |
| IMG_0124.JPG | 10/29/05 4:47:06 AM | 10/29/05 5:47:05 AM | 1 |
| IMG_0125.JPG | 10/29/05 4:47:10 AM | 10/29/05 5:47:11 AM | 1 |
| IMG_0126.JPG | 10/29/05 4:47:24 AM | 10/29/05 5:47:24 AM | 1 |
| IMG_0127.JPG | 10/30/05 2:34:20 AM | 10/30/05 4:34:20 AM | 2 |
| IMG_0128.JPG | 10/30/05 2:35:14 AM | 10/30/05 4:35:14 AM | 2 |
| IMG_0129.JPG | 10/30/05 2:36:06 AM | 10/30/05 4:36:05 AM | 2 |
| IMG_0130.JPG | 10/30/05 2:36:42 AM | 10/30/05 4:36:42 AM | 2 |
| IMG_0131.JPG | 10/30/05 2:36:54 AM | 10/30/05 4:36:55 AM | 2 |
| IMG_0132.JPG | 10/30/05 2:37:12 AM | 10/30/05 4:37:12 AM | 2 |
| IMG_0133.JPG | 10/30/05 2:37:44 AM | 10/30/05 4:37:45 AM | 2 |
| IMG_0134.JPG | 10/30/05 2:37:58 AM | 10/30/05 4:37:58 AM | 2 |
| IMG_0135.JPG | 10/30/05 2:38:00 AM | 10/30/05 4:38:00 AM | 2 |
| IMG_0136.JPG | 10/30/05 3:39:00 AM | 10/30/05 5:39:00 AM | 2 |
| IMG_0137.JPG | 10/30/05 3:39:06 AM | 10/30/05 5:39:06 AM | 2 |
| IMG_0138.JPG | 10/30/05 4:55:42 PM | 10/30/05 4:55:41 PM | 0 |
| IMG_0139.JPG | 10/30/05 4:55:52 PM | 10/30/05 4:55:51 PM | 0 |
| IMG_0140.JPG | 10/30/05 4:56:20 PM | 10/30/05 4:56:21 PM | 0 |
| IMG_0141.JPG | 10/30/05 4:56:46 PM | 10/30/05 4:56:46 PM | 0 |
| IMG_0142.JPG | 10/30/05 4:57:12 PM | 10/30/05 4:57:12 PM | 0 |
| IMG_0143.JPG | 10/30/05 6:01:08 PM | 10/30/05 6:01:08 PM | 0 |
| IMG_0144.JPG | 10/30/05 6:01:14 PM | 10/30/05 6:01:14 PM | 0 |
| IMG_0145.JPG | 10/30/05 6:01:20 PM | 10/30/05 6:01:19 PM | 0 |
| IMG_0146.JPG | 10/30/05 6:01:28 PM | 10/30/05 6:01:28 PM | 0 |

| | | | |
|---|---|---|---|
| IMG_0147.JPG | 10/30/05 6:02:08 PM | 10/30/05 6:02:08 PM | 0 |
| IMG_0148.JPG | 10/30/05 6:02:14 PM | 10/30/05 6:02:15 PM | 0 |
| IMG_0149.JPG | 10/30/05 6:02:22 PM | 10/30/05 6:02:22 PM | 0 |
| IMG_0150.JPG | 11/2/05 5:59:16 PM | 11/02/05 5:59:16 PM | 0 |
| IMG_0151.JPG | 11/2/05 5:59:26 PM | 11/02/05 5:59:25 PM | 0 |
| IMG_0152.JPG | 11/2/05 5:59:30 PM | 11/02/05 5:59:30 PM | 0 |
| IMG_0153.JPG | 11/2/05 5:59:34 PM | 11/02/05 5:59:34 PM | 0 |
| IMG_0154.JPG | 11/2/05 5:59:48 PM | 11/02/05 5:59:47 PM | 0 |
| IMG_0155.JPG | 11/2/05 6:00:22 PM | 11/02/05 6:00:22 PM | 0 |
| IMG_0156.JPG | 11/2/05 6:00:30 PM | 11/02/05 6:00:29 PM | 0 |
| IMG_0157.JPG | 11/2/05 6:00:38 PM | 11/02/05 6:00:38 PM | 0 |
| IMG_0158.JPG | 11/2/05 6:00:48 PM | 11/02/05 6:00:49 PM | 0 |
| IMG_0159.JPG | 11/2/05 6:01:10 PM | 11/02/05 6:01:10 PM | 0 |
| IMG_0160.JPG | 11/2/05 6:01:18 PM | 11/02/05 6:01:18 PM | 0 |
| IMG_0161.JPG | 11/2/05 6:09:00 PM | 11/02/05 6:08:59 PM | 0 |
| IMG_0162.JPG | 11/2/05 6:09:02 PM | 11/02/05 6:09:02 PM | 0 |
| IMG_0163.JPG | 11/2/05 6:09:10 PM | 11/02/05 6:09:11 PM | 0 |
| IMG_0164.JPG | 11/10/05 8:22:18 PM | 11/10/05 8:22:18 PM | 0 |
| IMG_0165.JPG | 11/10/05 8:22:30 PM | 11/10/05 8:22:30 PM | 0 |
| IMG_0168.JPG | 11/10/05 8:23:12 PM | 11/10/05 8:23:12 PM | 0 |
| IMG_0169.JPG | 11/10/05 8:23:26 PM | 11/10/05 8:23:26 PM | 0 |
| IMG_0172.JPG | 11/10/05 8:24:20 PM | 11/10/05 8:24:19 PM | 0 |
| IMG_0174.JPG | 11/10/05 8:24:48 PM | 11/10/05 8:24:47 PM | 0 |
| IMG_0175.JPG | 11/10/05 8:25:04 PM | 11/10/05 8:25:04 PM | 0 |
| IMG_0176.JPG | 11/10/05 8:25:10 PM | 11/10/05 8:25:11 PM | 0 |
| IMG_0177.JPG | 11/10/05 8:25:36 PM | 11/10/05 8:25:35 PM | 0 |
| IMG_0178.JPG | 11/10/05 8:25:54 PM | 11/10/05 8:25:54 PM | 0 |

| | | | |
|---|---|---|---|
| IMG_0179.JPG | 11/10/05 8:26:04 PM | 11/10/05 8:26:04 PM | 0 |
| IMG_0180.JPG | 11/10/05 8:26:22 PM | 11/10/05 8:26:22 PM | 0 |
| IMG_0181.JPG | 11/10/05 8:26:26 PM | 11/10/05 8:26:25 PM | 0 |
| IMG_0182.JPG | 11/10/05 8:26:30 PM | 11/10/05 8:26:29 PM | 0 |
| IMG_0183.JPG | 11/10/05 8:27:34 PM | 11/10/05 8:27:33 PM | 0 |
| IMG_0184.JPG | 11/24/05 9:07:50 PM | 11/24/05 9:07:50 PM | 0 |
| IMG_0185.JPG | 11/24/05 9:07:56 PM | 11/24/05 9:07:55 PM | 0 |
| IMG_0186.JPG | 11/24/05 9:08:08 PM | 11/24/05 9:08:07 PM | 0 |
| IMG_0187.JPG | 11/24/05 9:09:52 PM | 11/24/05 9:09:52 PM | 0 |
| IMG_0188.JPG | 11/24/05 9:10:08 PM | 11/24/05 9:10:08 PM | 0 |
| IMG_0189.JPG | 11/24/05 9:10:22 PM | 11/24/05 9:10:23 PM | 0 |
| IMG_0190.JPG | 11/24/05 9:10:28 PM | 11/24/05 9:10:28 PM | 0 |
| IMG_0191.JPG | 11/24/05 9:10:38 PM | 11/24/05 9:10:37 PM | 0 |
| IMG_0194.JPG | 12/18/05 12:37:58 AM | 12/18/05 12:37:58 AM | 0 |
| IMG_0197.JPG | 12/18/05 12:38:20 AM | 12/18/05 12:38:20 AM | 0 |
| IMG_0198.JPG | 12/18/05 12:38:28 AM | 12/18/05 12:38:28 AM | 0 |
| IMG_0199.JPG | 12/18/05 12:38:56 AM | 12/18/05 12:38:55 AM | 0 |
| IMG_0203.JPG | 12/25/05 2:59:44 AM | 12/25/05 2:59:44 AM | 0 |
| IMG_0204.JPG | 12/25/05 2:59:50 AM | 12/25/05 2:59:50 AM | 0 |
| IMG_0205.JPG | 12/25/05 3:00:42 AM | 12/25/05 3:00:42 AM | 0 |
| IMG_0206.JPG | 12/25/05 3:00:50 AM | 12/25/05 3:00:49 AM | 0 |
| IMG_0207.JPG | 12/25/05 3:01:40 AM | 12/25/05 3:01:40 AM | 0 |
| IMG_0208.JPG | 12/25/05 3:01:46 AM | 12/25/05 3:01:46 AM | 0 |
| IMG_0209.JPG | 12/30/05 5:56:06 PM | 12/30/05 5:56:05 PM | 0 |
| IMG_0210.JPG | 12/30/05 5:56:12 PM | 12/30/05 5:56:11 PM | 0 |
| IMG_0211.JPG | 12/30/05 5:56:16 PM | 12/30/05 5:56:15 PM | 0 |
| IMG_0212.JPG | 12/30/05 5:56:20 PM | 12/30/05 5:56:20 PM | 0 |

| | | | |
|---|---|---|---|
| IMG_0213.JPG | 12/30/05 5:56:46 PM | 12/30/05 5:56:46 PM | 0 |
| IMG_0214.JPG | 12/30/05 5:56:54 PM | 12/30/05 5:56:53 PM | 0 |
| IMG_0215.JPG | 12/30/05 5:56:56 PM | 12/30/05 5:56:56 PM | 0 |
| IMG_0216.JPG | 12/30/05 5:57:00 PM | 12/30/05 5:56:59 PM | 0 |
| IMG_0217.JPG | 12/30/05 5:58:50 PM | 12/30/05 5:58:50 PM | 0 |
| IMG_0218.JPG | 12/30/05 5:59:00 PM | 12/30/05 5:58:59 PM | 0 |
| IMG_0219.JPG | 12/30/05 5:59:08 PM | 12/30/05 5:59:07 PM | 0 |
| IMG_0220.JPG | 12/30/05 5:59:18 PM | 12/30/05 5:59:18 PM | 0 |
| IMG_0221.JPG | 12/30/05 5:59:56 PM | 12/30/05 5:59:56 PM | 0 |
| IMG_0222.JPG | 12/30/05 6:00:08 PM | 12/30/05 6:00:08 PM | 0 |
| IMG_0223.JPG | 12/30/05 6:00:24 PM | 12/30/05 6:00:24 PM | 0 |

## Appendix C: Analysis of Files Carved from HDD and CF Card

The content of four digital photos, IMG_0180 through IMG_0183, are the only ones that are exactly the same across both the CF card (GX 521A) and the external hard drive (GX 503), meaning they are the only photos whose file names and MD5 hashes match. Initially, this was **discovered by comparing the file hashes from two file listings, "CF card listing.csv" and "File** Listing of Backup Folder (BKP.DellDimension8300-20090330).csv," **derived from the FBI's FTK** reports.

In addition, I inspected two additional **file listings, "GX 521A Replacement (carved files)_2019_06_11.csv" and "Full File Listing of Hard Drive Contents (GX 503).csv," which** provided items *carved* from the CF card and external hard drive, respectively. In these listings I discovered a suspicious relationship between photos IMG_0180 through IMG_0183 and four other photos on the CF card, IMG_0093, IMG_0094, IMG_0096, and IMG_0097, respectively.

Before I describe those relationships, however, it would be helpful for the reader to understand how carved files are generated. Figure 1 represents a digital photograph named **IMG_0180.JPG**, which has a file size of 2,539,833 bytes (about 2.5 MB). The logical portion of the file consists of three primary components.

- **EXIF data**, which typically contains camera-generated metadata, is fixed length and occupies the first portion of the file from byte offset 0 to offset 9728.
- The second portion of the file is the picture **thumbnail**, a variable-length component that occupies the space between the end of the EXIF data (offset 9728) and the beginning of the main picture (offset 16845). Subtracting these two numbers provides the file size of the thumbnail, 7,117 bytes. When a forensic tool carves it from the parent file it is given the **file name "Carved [9728].jpeg," indicating its starting location in the file.**
- The third portion of the file is the **main picture**, occupying the largest portion of the file at 2,522,988 bytes. Since the main picture begins at byte offset 16845, the carving forensic tool will give it a fi**le name of "Carved [16845].jpeg."**


**Figure 1. How a forensic tool creates and names files carved from digital photographs.**

For brevity I will limit the discussion of the suspicious files (IMG_0093, IMG_0094, IMG_0096, and IMG_0097) to the relationship between IMG_0093 and IMG_0180. The corresponding relationships between IMG_0094, IMG_0096, IMG_0097 and IMG_181, IMG_182, IMG_183, respectively, are identical.

Table 1 below was excerpted from "Full File Listing of Hard Drive Contents (GX 503).csv" and displays information about IMG_0093 and IMG_0180. As discussed elsewhere, the Created dates do not make sense. That anomaly aside, however, the file size information is consistent. For example, for each file the logical size (L-Size) added to the size of its corresponding FileSlack is equal to the physical size (P-size), as it should. Also, each of these files have corresponding carved files, including "Carved [9728].jpeg," which is a thumbnail picture carved starting at byte offset 9728. With a single exception - as explained previously - the thumbnail files for each digital photograph in this case can be identified by the name "Carved [9728].jpeg." A second carved file, "Carved [XXXXX].jpeg," which is the main picture carved starting at byte offset XXXXX, will vary with each photo because thumbnail sizes are different. The table below demonstrates that subtracting the two starting byte offsets for the carved files (in **red**) predictably results in the logical size for the thumbnail (in **blue**).

| Row | Name | Category | Created | Accessed | Modified | P-Size (bytes) | L-Size (bytes) | MD5 |
|---|---|---|---|---|---|---|---|---|
| 1 | **IMG_0093.JPG** | JPEG EXIF | 7/26/2003 11:06 | 2/12/2010 | 10/19/2005 15:33 | 2523136 | 2500404 | 697cec1244dce21ecc4f82cd3a764644 |
| 2 | IMG_0093.JPG.File Slack | Slack Space | n/a | n/a | n/a | 22732 | 22732 | |
| 3 | Carved [**14844**].jpeg | JPEG | n/a | n/a | n/a | n/a | 2485560 | ae6cbe511c9f3bdec52917e3dca05129 |
| 4 | Carved [**9728**].jpeg | JPEG | n/a | n/a | n/a | n/a | **5116** | 51202a6c4b8e6084f15345656156481c |
| **5** | **IMG_0180.JPG** | JPEG EXIF | 7/26/2003 11:06 | 2/12/2010 | 11/10/2005 17:26 | 2555904 | 2539833 | f6202d0b41e30c7c21aeae32c38baf9b |
| 6 | IMG_0180.JPG.File Slack | Slack Space | n/a | n/a | n/a | 16071 | 16071 | |
| 7 | Carved [**16845**].jpeg | JPEG | n/a | n/a | n/a | n/a | 2522988 | b991eaa84b4d91dfa2d0eece1e902430 |
| 8 | Carved [**9728**].jpeg | JPEG | n/a | n/a | n/a | n/a | **7117** | 6babe3f7c2bd2c6c73d15e3d2db42a95 |

**Table 1. Excerpt from "Full File Listing of Hard Drive Contents (GX 503).csv."**

Next we turn our attention to an excerpt from "GX 521A Replacement (carved files)_2019_06_11.csv," which also displays information about IMG_0093 and IMG_0180 - but on the CF card. There are several inconsistencies with this data (See Table 2).

- The file named "Carved [2129920].jpeg" indicates the file was carved from **IMG_0093** starting at byte offset 2129920. This would mean the file would have been carved starting near the *end* of the digital photo file, which has a logical size of 2500404 bytes according to the previous table. There was no file size data present in this file listing (which is suspicious in itself). However, subtracting 2129920 from 2500404 yields a maximum file size of 370484 bytes for this carved file, which is too large to be a thumbnail and too small to be the main picture data for the photo.
- In row 2 a file named "Carved [16845].jpeg" indicates the file was carved from "Carved [2129920].jpeg" (which was itself carved from IMG_0093) starting at byte offset 16845. Surprisingly, this is **precisely the same byte offset** that began the main picture carving in **IMG_0180** as shown in this table (row 5) and verified in the previous table by a matching MD5 hash (See Table 1, row 7).
- As discussed earlier, files in this case named "Carved [9728].jpeg" are thumbnails that are carved from their parent photo files starting at byte offset 9728. However, the **same thumbnail** (with matching hashes) was **carved from two different files**, **IMG_0093** and **IMG_0180**. (See Table 2, rows 3-4 and compare at Table 1, row 8).

| Row | Path | Hash | Name | Deleted? |
|---|---|---|---|---|
| 1 | /DCIM/100CANON/**! MG_0093.JPG**»Carved [2129920].jpeg | 8514c14257901fca23dab82db71f6c0c | ! MG_0093.JPG»Carved [2129920].jpeg | Y |
| 2 | /DCIM/100CANON/**! MG_0093.JPG**»Carved [2129920].jpeg»Carved [**16845**].jpeg | d4831cccb7f5ac74632cc09a32d28515 | ! MG_0093.JPG»Carved [2129920].jpeg»Carved [16845].jpeg | Y |
| 3 | /DCIM/100CANON/**! MG_0093.JPG**»Carved [2129920].jpeg»Carved [**9728**].jpeg | 6babe3f7c2bd2c6c73d15e3d2db42a95 | ! MG_0093.JPG»Carved [2129920].jpeg»Carved [9728].jpeg | Y |
| 4 | /DCIM/101CANON/**! MG_0180.JPG**»Carved [**9728**].jpeg | 6babe3f7c2bd2c6c73d15e3d2db42a95 | ! MG_0180.JPG»Carved [9728].jpeg | Y |
| 5 | /DCIM/101CANON/! MG_0180.JPG»Carved [**16845**].jpeg | b991eaa84b4d91dfa2d0eece1e902430 | ! MG_0180.JPG»Carved [16845].jpeg | Y |

**Table 2. Excerpt from "GX 521A Replacement (carved files)_2019_06_11.csv" (second listing for the CF card, with no file sizes present).**

As mentioned previously, the same pattern appears in the file listings for relationships between IMG_0094 and IMG_0181, IMG_0096 and IMG_0182, and IMG_0097 and IMG_0183. Two additional observations point to IMG_0093, IMG_0094, IMG_0096, and IMG_0097 being counterfeit files on the CF card:

- With the exception of unallocated space, the files IMG_0093, IMG_0094, IMG_0096, and IMG_0097 are the only files in the CF card file listing with apparent nested carving (carving from carved files).
- Unlike the consistency of files IMG_0180 to IMG_0183, the byte offset data and MD5 hashes of files IMG_0093, IMG_0094, IMG_0096, and IMG_0097 are NOT consistent between Tables 1 and 2 (i.e., between the hard drive and CF card).

**Other anomalous behavior**

Additional analyses of the CF card and WD HDD file listings reveal bizarre patterns that support the finding that files were altered and transferred between devices:

- A group of files located on the WD HDD were given **nonstandard file names**, from IMG_0059-1 to IMG_0070-1. Neither the 04/11/2019 nor the 06/11/2019 CF card file listings contain any record of these photos existing on the CF card, despite their camera-related EXIF data being identical to all the others. Notably, these names were not assigned automatically by the camera, but were rather created by a user action, thus proving at least one aspect of metadata editing.
- The CF card file listing shows large swaths of missing file name sequences, and sequences with no content, punctuated by groups of 5-6 files with recoverable content (see Table 3). This is not consistent with normal use of a camera, where the user might review and choose to occasionally delete unwanted photographs as desired. Rarely would this deletion activity follow such a distinctive pattern as what appears in the file listing. However, the pattern would be consistent with someone copying photos between the CF card and an unknown computer.

| Name | Deleted | Created | Accessed | Modified | Hash | Path |
|---|---|---|---|---|---|---|
| IMG_0089.JPG | Y | 10/19/2005 18:56 | 10/19/2005 | 10/19/2005 18:56 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0090.JPG | Y | 10/19/2005 19:32 | 10/19/2005 | 10/19/2005 19:32 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0091.JPG | Y | 10/19/2005 19:32 | 10/19/2005 | 10/19/2005 19:32 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0092.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0093.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 04e96f3f0f48c3b117cbf4bcd516a857 | Lexar CF 2GB Card/I |
| IMG_0094.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 97d26874707bf3f97e76fc22b57d86d0 | Lexar CF 2GB Card/I |
| IMG_0095.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 81f59288eb1ca3ce02826f1ce46dc4d5 | Lexar CF 2GB Card/I |
| IMG_0096.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 884764bfbb7a72ed5f726af5d5eb11b5 | Lexar CF 2GB Card/I |
| IMG_0097.JPG | Y | 10/19/2005 19:33 | 10/19/2005 | 10/19/2005 19:33 | 5cb3245ec43bf2d9b0e373995336deee | Lexar CF 2GB Card/I |
| IMG_0098.JPG | Y | 10/19/2005 19:34 | 10/19/2005 | 10/19/2005 19:34 | 452db09a0de54234504bb1211f6c30eb | Lexar CF 2GB Card/I |
| IMG_0099.JPG | Y | 10/20/2005 16:20 | 10/20/2005 | 10/20/2005 16:20 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0100.JPG | Y | 10/20/2005 16:20 | 10/20/2005 | 10/20/2005 16:20 | NO HASH | Lexar CF 2GB Card/I |
| GAP - Alleged contraband images 0150-0163 do not appear here at all | | | | | | |
| IMG_0172.JPG | Y | 11/10/2005 20:24 | 11/10/2005 | 11/10/2005 20:24 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0173.JPG | Y | 11/10/2005 20:24 | 11/10/2005 | 11/10/2005 20:24 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0174.JPG | Y | 11/10/2005 20:24 | 11/10/2005 | 11/10/2005 20:24 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0175.JPG | Y | 11/10/2005 20:25 | 11/10/2005 | 11/10/2005 20:25 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0176.JPG | Y | 11/10/2005 20:25 | 11/10/2005 | 11/10/2005 20:25 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0177.JPG | Y | 11/10/2005 20:25 | 11/10/2005 | 11/10/2005 20:25 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0178.JPG | Y | 11/10/2005 20:25 | 11/10/2005 | 11/10/2005 20:25 | NO HASH | Lexar CF 2GB Card/I |
| IMG_0179.JPG | Y | 11/10/2005 20:26 | 11/10/2005 | 11/10/2005 20:26 | ab069f934603db10d2b579a5323a117c | Lexar CF 2GB Card/I |
| IMG_0180.JPG | Y | 11/10/2005 20:26 | 11/10/2005 | 11/10/2005 20:26 | f6202d0b41e30c7c21aeae32c38baf9b | Lexar CF 2GB Card/I |
| IMG_0181.JPG | Y | 11/10/2005 20:26 | 11/10/2005 | 11/10/2005 20:26 | c22d37f14011b042388917706a89c4a9 | Lexar CF 2GB Card/I |
| IMG_0182.JPG | Y | 11/10/2005 20:26 | 11/10/2005 | 11/10/2005 20:26 | 550df2c454f2c70cc0911f6ceaad4549 | Lexar CF 2GB Card/I |
| IMG_0183.JPG | Y | 11/10/2005 20:27 | 11/10/2005 | 11/10/2005 20:27 | b0d057b32850bfc7c20674f7dfa1ae3a | Lexar CF 2GB Card/I |
| GAP - Alleged contraband images 0184-0191 do not appear here at all | | | | | | |
| IMG_0193.JPG | Y | 12/19/2005 0:37 | 12/19/2005 | 12/19/2005 0:37 | NO HASH | Lexar CF 2GB Card/I |

**Table 3. Analysis showing conspicuous gaps in data appearing in the CF card file listing.**

**Summary**

According to the file paths and hash values I observed, the carving byte offset data and thumbnails are exactly the same in two sets of files purported to be different. To be clear, two different digital photographs would *never* share exactly the same thumbnail picture. It is impossible without manual intervention. Moreover, the photographs IMG_0093, IMG_0094, IMG_0096, and IMG_0097, produced multiple, duplicate carved files, which on flash media is indicative of file modification. By contrast, all the other files on the CF card file listing contain exactly two carved files: a "Carved [9728].jpeg" and a carved main picture named "Carved [XXXXX].jpeg."

Given the above facts, I believe the following actions describe the most plausible explanation for what I observed with regard to the eight files in question.

These four files (IMG_0180 through IMG_0183) were either manually copied from an unknown computer to the CF card or else were copied from the CF card to the unknown computer, where they were "backed up" to the external hard drive. This action would explain the fact that these four files (the only four of about 200) actually matched hashes between devices. Also, it is likely that someone copied another version of these *same four files* to the CF card, altered their content, and renamed them to IMG_0093, IMG_0094, IMG_0096, and IMG_0097. These actions would

explain 1) why these files bear no resemblance to those on the hard drive with the same file names, 2) why they contain the identical thumbnail pictures and common starting byte offsets as those contained in the IMG_0180 to IMG_0183 files, 3) why there are multiple, carved instances of these files on the flash media, and 4) why none of these files appeared on the 04/11/2019 CF card file listing while appearing on the subsequent 06/11/2019 file listing. There are no plausible natural or automated causes to explain such phenomena.

In summary, the forensic evidence demonstrates that alterations were intentionally made to files on the CF card, and the differences between the 04/11/2019 and 06/11/2019 file listings suggest those alterations took place while the CF card was in the custody of the FBI, as the devices were collected on March 27, 2018.

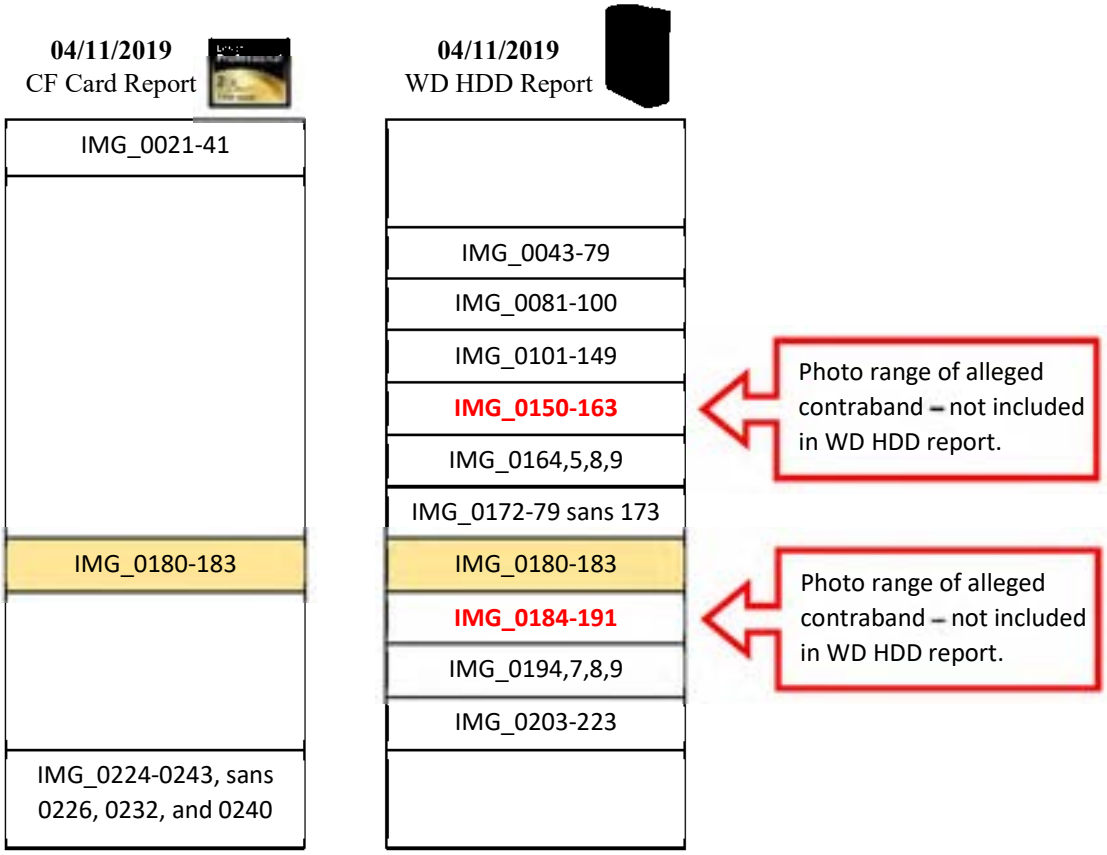
# Appendix D: Description of New Files Appearing on the FBI's Forensic Report Between 04/11/2019 and 06/11/2019

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

**Introduction:**

In the present case, U.S. vs KEITH RANIERE, the FBI completed two forensic examinations and generated two different reports on the same piece of evidence: A compact flash (CF) card found in a digital camera case. The Government claimed that digital photographs from this CF Card were eventually backed up to a Western Digital hard disk drive (WD HDD), which also contained alleged child pornography. **The government's narrative depended on** creating a strong connection between the CF Card, allegedly belonging to the defendant, and the WD HDD that supposedly backed up photos from the CF Card. This brief analysis offers a plausible explanation for why a second examination, and a second report of the CF Card, were generated by an FBI forensic examiner (FE)[1].

## Figure 1: Files Appearing on the First FBI Forensic Reports of the CF Card and WD HDD

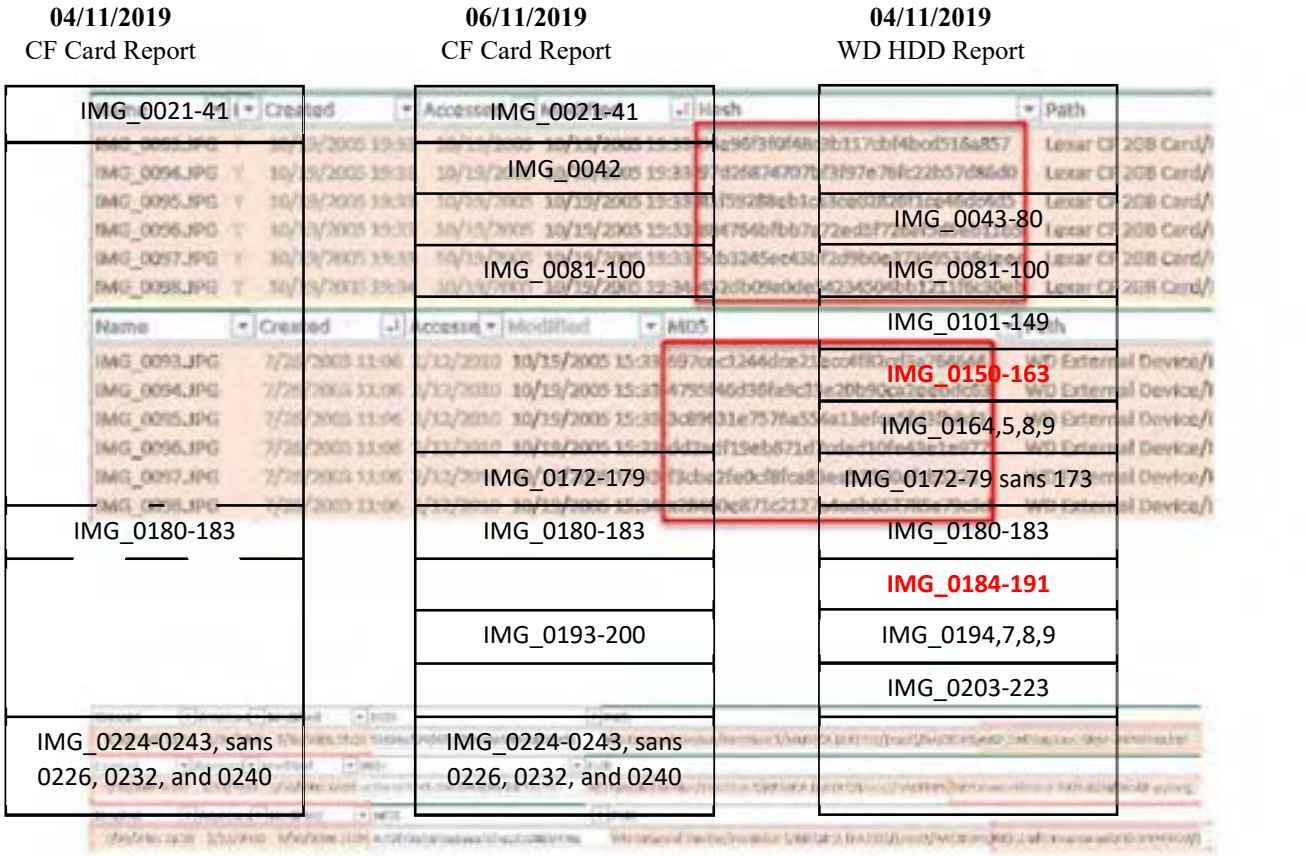



**Observations:**

- Both forensic reports were generated on the same day, **April 11, 2019**.
- The **CF Card report** was created by **FE Stephen Flatley**, who kept the CF Card until 06/07/2022.
- The **WD HDD report** was created by **FE Brian Booth**, using a forensic copy made by his trainee.
- Only **four photos**, named IMG_0180-183, are common to both forensic reports (highlighted yellow).
- At this time **no other files** on the CF Card report could be shown to be **"backed up" to the WD HDD**.

[1] **For more information about the background of the case and the Government's narrative presented at trial, please see my** full reports detailing Technical and Process Findings.

**Figure 2: Generating the Second FBI Forensic Report on the CF Card (June 11, 2019)**




**Observations:**

As documented in the Chain of Custody, SA Mills delivered the CF Card, in an **unsealed bag**, to FE Booth on 06/10/2019, during the last week of trial and more than **14 months** after the search team had collected it. SA Lever requested that FE Booth complete a **new examination** and a **"replacement"** (dated 06/11/2019 in the above figure).

**None** of the new files appearing on the 06/11/2019 report (shaded green) was viewable in the report. No explanation was provided for the appearance of the new files or why they were **unviewable**.

**All** the previous CF Card files (in white) are viewable in both CF Card reports.

It is extremely unlikely that **eight of the new files** on the 6/11 CF Card report (IMG_0172-179) just happen to occupy the filename space before the small group of **"**common**"** photos (IMG_0180-183) and then **another eight new files** (IMG_0193-200) just happen to appear right after the alleged contraband photo range (IMG_0184-191), which themselves just happen to appear immediately after the common photos.

The **alleged contraband** photos, IMG_0150-163 and IMG_0184-191, appear in neither of the CF Card reports. **If the government's narrative** as correct, then one would reasonably expect some remnants of these photos **to have** **the** **reports.**

IMG_0042 appears **only** on the 6/11 CF Card report – so it seems to fill a filename **"gap."**

- IMG_0021-0041 appear on the 4/11 CF Card report but not on the WD HDD report.
- IMG_0043-0179 appear on the WD HDD report but not on the 4/11 CF Card report.

The new file ranges on the 6/11 report are **uninterrupted**. Unlike the WD HDD report, there are no missing file names or gaps within each group of new files.

**Figure 3: Evidence Supporting the Addition of New Files to the CF Card**

| | | |
|---|---|---|
| IMG_0079.JPG | 10/19/05 2:54 PM | /Msk101905/2005-10-19-0727-59/IMG_0079.JPG |
| IMG_0080.JPG | 10/19/05 2:54 PM | /Msk101905/2005-10-19-0727-59/IMG_0080.JPG |
| IMG_0081.JPG | 10/19/05 2:54 PM | /Msk101905/2005-10-19-0727-59/IMG_0081.JPG |
| IMG_0082.JPG | 10/19/05 2:54 PM | /Msk101905/2005-10-19-0727-59/IMG_0082.JPG |
| IMG_0083.JPG | 10/19/05 2:55 PM | /Msk101905/2005-10-19-0727-59/IMG_0083.JPG |
| IMG_0084.JPG | 10/19/05 2:55 PM | /Msk101905/2005-10-19-0727-59/IMG_0084.JPG |
| IMG_0085.JPG | 10/19/05 2:55 PM | /Msk101905/2005-10-19-0727-59/IMG_0085.JPG |
| IMG_0086.JPG | 10/19/05 2:55 PM | /Msk101905/2005-10-19-0727-59/IMG_0086.JPG |
| IMG_0087.JPG | 10/19/05 2:56 PM | /Msk101905/2005-10-19-0727-59/IMG_0087.JPG |
| IMG_0088.JPG | 10/19/05 2:56 PM | /Msk101905/2005-10-19-0727-59/IMG_0088.JPG |
| IMG_0089.JPG | 10/19/05 2:56 PM | /Msk101905/2005-10-19-0727-59/IMG_0089.JPG |
| IMG_0090.JPG | 10/19/05 3:32 PM | /Df101905/2005-10-19-0727-57/IMG_0090.JPG |
| IMG_0091.JPG | 10/19/05 3:32 PM | /Df101905/2005-10-19-0727-57/IMG_0091.JPG |
| IMG_0092.JPG | 10/19/05 3:33 PM | /Df101905/2005-10-19-0727-57/IMG_0092.JPG |
| IMG_0093.JPG | 10/19/05 3:33 PM | /Df101905/2005-10-19-0727-57/IMG_0093.JPG |
| IMG_0094.JPG | 10/19/05 3:33 PM | /Df101905/2005-10-19-0727-57/IMG_0094.JPG |
| IMG_0095.JPG | 10/19/05 3:33 PM | /Df101905/2005-10-19-0727-57/IMG_0095.JPG |
| IMG_0096.JPG | 10/19/05 3:33 PM | /Df101905/2005-10-19-0727-57/IMG_0096.JPG |
| IMG_0097.JPG | 10/19/05 3:33 PM | /Df101905/2005-10-19-0727-57/IMG_0097.JPG |
| IMG_0098.JPG | 10/19/05 3:34 PM | /Df101905/2005-10-19-0727-57/IMG_0098.JPG |
| IMG_0099.JPG | 10/20/05 12:20 PM | /Mnp102005/2005-10-20-0640-31/IMG_0099.JPG |
| IMG_0100.JPG | 10/20/05 12:20 PM | /Mnp102005/2005-10-20-0640-31/IMG_0100.JPG |
| IMG_0101.JPG | 10/20/05 12:20 PM | /Mnp102005/2005-10-20-0640-31/IMG_0101.JPG |
| IMG_0102.JPG | 10/20/05 12:21 PM | /Mnp102005/2005-10-20-0640-31/IMG_0102.JPG |
| IMG_0103.JPG | 10/20/05 12:21 PM | /Mnp102005/2005-10-20-0640-31/IMG_0103.JPG |
| IMG_0104.JPG | 10/20/05 12:25 PM | /Mnp102005/2005-10-20-0640-31/IMG_0104.JPG |
| IMG_0105.JPG | 10/20/05 12:26 PM | /Mnp102005/2005-10-20-0640-31/IMG_0105.JPG |
| IMG_0106.JPG | 10/20/05 12:27 PM | /Mnp102005/2005-10-20-0640-31/IMG_0106.JPG |
| IMG_0107.JPG | 10/20/05 12:49 PM | /Mnp102005/2005-10-20-0640-31/IMG_0107.JPG |
| IMG_0108.JPG | 10/20/05 12:49 PM | /Mnp102005/2005-10-20-0640-31/IMG_0108.JPG |

Why were **only the last nine photos** (not the first two) from **Msk101905** added to the new 6/11 CF Card Report?

Photo files shaded in green were added to the **06/11** CF Card report and did not appear on the **4/11** report.

Why were **only the first two photos** (not the last eight) from **Mnp102005** added to the new 6/11 CF Card Report?

**Observations:**

- The above file listing was adapted from the WD HDD report, so **all** these files appear **in the "backup"** drive.
- **None** of these files appear on the 4/11 CF Card report.
- Files shaded in **green** appear on the 6/11 CF Card report, but none of them are viewable on that report.
- Files with a **red** boundary were located **in the WD HDD's** Msk101905 folder.
- Files with a **blue** boundary were located **in the WD HDD's** Mnp102005 folder.
- It is **extremely unlikely** that photos would have been saved to and deleted from the CF Card in this manner as a result of normal user behavior (See Implications discussion below).

## Implications

As explained elsewhere, the Government claimed that digital photos, including **alleged contraband**, had been created with a Canon camera, saved to **the camera's CF card, transferred to an unknown computer, and then backed** up to the WD HDD. **Figure 1** illustrates the initially weak relationship between files on the CF card and the alleged **"backup" of those** files contained in the WD HDD. In fact, **according to the FBI's report** on 04/11/2019, **only four photographs** were reported as being common to both devices.

In **Figure 2**, however, the introduction of **new files to the FBI's 06/11/2019 "replacement"** forensic report creates an obviously stronger relationship between the devices. In all, 37 photos with filenames matching those on the WD HDD were added to the 06/11/2019 report in small, contiguous groups of files. Unfortunately **–** or perhaps, *conveniently* **– none of the new files were viewable** as photographs in the second report. As a result, none of the new files could be verified visually or forensically against their namesakes on the WD HDD report.[2] The FBI never provided an explanation for the appearance of new photos on the 06/11/2019 report or why they were the only photos on the CF card that were not viewable in the report.

**Figure 3** requires a more robust explanation. In the case of the new files **IMG_0081-100** (highlighted in green), it seems that someone decided to **add the appearance of those 20 files** using round start and end **file numbers –** but without regard for the three separate **folders** into which their namesakes would eventually be discovered on the WD HDD **"backup."** To accept the integrity and completeness of the 6/11 CF Card report, one must believe that the user:

- Took photos IMG_0079-89 on the CF Card,
- Saved the eleven photos to the Msk101905/2005-10-19-0727-59 folder on the unknown computer,
- Returned to the CF Card and *securely* deleted[3] the only the first two photos in that series (IMG_0079-80),
- Took photos IMG_0099-108 on the CF Card,
- Saved the ten photos to the /Mnp102005/2005-10-20-0640-31 folder on the unknown computer, and
- Returned to the CF Card and *securely* deleted **all BUT** the first two photos in the series (IMG_0099-100).

Such a creating, saving and deleting behavior is extremely unlikely (securely deleting from the camera only the first two photos in one series and all BUT the first two photos in a subsequent series). That the user would just happen to selectively curate and delete photos with consecutive filenames like this **–** based on content **–** is not a reasonably credible scenario.

A more plausible explanation is that someone with physical control of the CF Card:

- Recognized the **weak relationship** between the photos reported on the 04/11/2019 CF Card report and those reported as **"backup" files on the WD HDD,** including alleged contraband,
- Examined the file listing of the WD HDD and chose a convenient range based on **filenames** (IMG_0081-100) rather than their saved **folders**,
- **Created the appearance** (through file and metadata manipulation) that those files had been discovered on the CF Card as reported on the 06/11/2019 report, and
- Botched the file creation and deletion of the new files, rendering them **unviewable** in the 06/11/2019 report.

---

[2] The Modified date/time stamps between the new files in the 06/11/2019 report and their namesakes on the WD HDD did match. However, as explained in my report of Technical Findings, such metadata is easily changed and in this case it was obviously manipulated, enhancing the CF Card **–** WD HDD relationship required by the Government's narrative.

[3] By *securely deleted* I refer to the process of selectively overwriting physical sectors on the media so that the files cannot be recovered by forensic tools. Selectively eradicating photos in this way is not something a normal user would be able to accomplish. If the deleted photos were recoverable, then the FBI would have included them in the second CF card report.

**Conclusion:**

The defense team was **provided the FBI's forensic report of the CF Card generated on 04/11/2019 and then the second "replacement"** report, which was generated on 06/11/2019 and contained 37 additional files.

Along with the appearance of new files on a second CF Card forensic report, it is also undisputed that the **contents of the CF card were modified** on 09/19/2018, while in FBI custody, and that the CF card was delivered to FE Brian Booth in an **unsealed** cellophane bag just two days before FE Booth took the stand.[4] Therefore, in my expert opinion all indications of means, motive, and opportunity point to FBI employees **creating the appearance of additional files** on the CF Card in order to substantiate a relationship between the CF Card and the WD HDD containing the alleged contraband.

[4] These two facts were verified by FE Brian Booth in his sworn testimony.

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

# Summary of Process Findings

**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 (See attached CV). 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 an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

**Review of Evidence**

My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports generated by members of the FBI's Computer Analysis Response Team (CART). Based on my review, I have observed several technical, administrative, and evidence handling irregularities that raise serious concerns about the integrity of the evidence. Specifically, in this paper I describe violations of processes and procedures which occurred in this case and that likely affected the outcome at trial.

**Key Findings**

**Finding 1: Receiving unsealed evidence created a broken Chain of Custody.**

- Neither the camera (Court transcript, p. 4886) nor the CF card (p.4889) was sealed when delivered to CART Forensic Examiner (FE) Brian Booth on 06/10/2019, two days before he took the stand. The FBI Chain of Custody for the CF card (DX 945) indicates that at least three FBI employees – FE Stephen Flatley, SA Elliot McGinnis, and SA Christopher Mills – had physical control of the evidence from the date a reexamination was requested (06/07/2019) to the date it was delivered to FE Booth in an unsealed package (06/10/2019).
- FE Booth's exam notes (DX 961) make no mention of the chain of custody, or of the fact that he received the evidence in unsealed packaging, although in court he admitted it was unsealed when he received it (p.4886 and p.4905). As I will discuss later, FBI policy requires the securing and sealing of evidence, and employees may be disciplined if they fail to do so. In my experience with the FBI, I never received unsealed evidence other than in exigent (emergency) situations.

**Finding 2: FBI employees engaged in unusual evidence handling procedures.**

- **What normal looks like:** Large FBI offices like the New York Division, where the evidence was processed, have a centralized evidence control and storage facility sometimes referred to as the Evidence Control Unit (ECU). Normally, evidence is collected at a search site by the case agent or a designated seizing agent, and a description of the collected items is entered into Sentinel, the FBI's case management system. Then the agent has up to ten days to physically turn over the evidence to Evidence Control with the chains of custody. After the case agent submits a written request to have the evidence examined, the assigned CART examiner would check out the relevant evidence items from Evidence Control and sign the chains of custody. In her notes (DX 961), Forensic Examiner Trainee (FET) Virginia Donnelly recorded multiple instances where she created derivative evidence items (forensic copies, extractions, and backups of the originals) and turned them into Evidence Control. This is also normal.
- **Abnormalities in this case:** The digital evidence seized on 03/27/2018 seemed to be in and out of the physical control of the case agents, rather than primarily managed through the ECU as described above. Although the evidence was first turned into ECU by the ten-day deadline, it was subsequently checked out by individuals who were not authorized to review digital evidence. The chain of custody for the Camera and CF Card, for example, indicate that the evidence was checked out by SA Maegan Rees on 07/10/2018 for 17 days and by SA Michael Lever 09/19/2018 for seven days – before it was first examined by a CART examiner on 02/22/2019. Both SA Rees and SA Lever indicated "Review" as the reason they were checking the evidence out of the ECU, but **neither of these individuals were authorized to review the contents of unexamined digital evidence**[1].
- Based on my own experience, a case agent would leave digital evidence in the ECU until a CART examiner is requested to check out and examine the evidence. For digital evidence, there is no good reason to check it out of Evidence Control, because the case agent cannot possibly gain any investigative benefit from retaining evidence that he or she cannot examine.
- According to the Chain of Custody for the WD HDD (DX 960), the last person to accept custody of the device was SA Michael Lever, who checked it out from ECU on 02/22/2019. The reason SA Lever provided was "SW," presumably meaning "search warrant," but it is unknown what actions SA Lever took on the WD HDD, or who took custody of the device when he was finished with it. Although the WD HDD had been forensically imaged (copied) by FET Donnelly on 09/19/2018 and processed on 09/24/2018, FE Booth did not generate a report of its contents until 04/11/2019.

[1] In their report regarding the Lawrence Nassar case, the DOJ/OIG made public certain information regarding the FBI's evidence handling procedures: "According to the FBI's Field Evidence Management Policy Guide, evidence must be documented into the FBI Central Recordkeeping System no later than 10 calendar days after receipt. Similarly, the Digital Evidence Policy Guide states that, 'Undocumented, "off the record" searches or reviews of [digital evidence] are not permitted'" (p. 13). (https://oig.justice.gov/sites/default/files/reports/21-093.pdf)

- Finally, FE Booth's examination notes (DX 961) end abruptly after he created a forensic copy of the CF card. Strangely absent from his notes are the options he chose while processing the data with AD Lab, the generation of the "replacement FTK report" presented at trial or the final disposition of the original or derivative evidence. Such details would complete a normal CART forensic report.

**Finding 3: The CF Card was accessed by an unauthorized FBI employee.**

- According to the FTK reports, the last Accessed dates for active files on the CF card was 09/19/2018 – six months after the CF was collected by investigators and five months before it was first delivered to an authorized CART examiner.
- According to FBI Chain of Custody for the Camera and CF Card (DX 945), the FBI employee who had physical control over the CF card between 09/19/2018 and 09/26/2018 was SA Michael Lever, who recorded "Evidence Review" as his reason for accepting custody (see my Technical Findings report). SA Lever was the primary case agent and not a CART examiner, meaning he was not authorized to review the unexamined digital evidence.
- The FBI's Digital Evidence Policy Guide expressly prohibits any "Undocumented, 'off the record' searches or reviews of digital evidence" and permits investigators to review digital evidence only after it has been processed by an authorized method.[2]
- According to the same Chain of Custody, SA Maegan Rees had previously checked out the Camera and CF card for "Review" on 07/10/2018 and kept them for 17 days. She is also not a CART examiner and also would be prohibited from reviewing unexamined digital evidence. However, if she did access the CF card without a write blocker, then the last Accessed dates would have been overwritten two months later by the actions of SA Lever, who did access the CF card without a write blocker.
- Therefore, there is no doubt the CF card was accessed by at least one unauthorized FBI employee using an unauthorized process.

**Finding 4: The CF Card was altered at least once, and likely twice, while in FBI Custody**.

- **On 9/19/2018:** File system dates were overwritten on the CF card on at least one occasion, on 09/19/2018, while in FBI custody. This means, at a minimum, that the CF card was accessed without the use of a write blocking device. Failing to preserve digital evidence against alteration is an automatic fail in many of the FBI forensics classes I have taught because write blocking is a critical procedure that, if skipped, becomes an admissibility issue in court.
- **Between 4/11/2019 and 6/11/2019**: According to an FTK forensic report of the CF card completed on 4/11/2019 by "srflatley" (FE Stephen Flatley) and another report completed

[2] *Ibid*, p.13. See also p. 83: "according to the FBI's Removable Electronic Storage Policy Directive, employees may not connect non-FBI removable electronic storage, such as a thumb drive, to FBI equipment without authorization."

on 6/11/2019 by "bsbooth" (FE Brian Booth), several files appeared on the second report that were not included on the first report. For reasons I described in my Technical Findings report (see Technical Findings #1 and #2), there is a high likelihood the new files were added to the CF card and altered between these dates. In Appendix D of my Technical Findings report, I explained why adding new files to the CF card could have been used to support the government's narrative regarding the origin of photos on the WD HDD device.[3]

- The difference between the FTK reports cannot be attributed to the use of a different tool, because both examiners used the same tool and version number: AccessData Forensic Toolkit, Version 6.3.1.26.

**Finding 5: The FBI Expert Witness knowingly gave false testimony.**

- **FE Booth testified that receiving unsealed evidence is not extraordinary (p. 4887).** This characterization by Booth is false, as all CART examiners are trained to receive evidence that has been sealed and initialed.[4] According to FBI evidence handling protocols, anytime a seal is broken on evidence, it must be resealed with a date and initials before relinquishing it to the next person in the chain of custody.[5]
- **FE Booth testified he did not know who had the evidence prior to his examination – two days prior to his testimony.** When he was asked, "And who was it that had access to the camera or the box prior to the time of your examination of it?" FE Booth answered, "I don't have that evidence sheet in front of me to be able to refer" (p. 4889). As mentioned previously, according to FE Booth's examination notes (DX 961), it was the "Case Agent" (but in fact SA Mills) who gave Booth the unsealed camera and CF card on 06/10/2019. It is not credible that FE Booth after two days could have forgotten the person who gave him the one piece of evidence he processed alone during the case.
- **FE Booth repeatedly testified to the reliability of EXIF data,** and that it is "very hard to remove," (p. 4819) and "it's not easily modifiable" (p. 4830). In fact, there are several readily available tools that can easily modify EXIF data. This is a fact that would be well-known to any forensic examiner (see **Appendix A** for a white paper I wrote demonstrating – with screen shots – how easy it is to modify EXIF data). Also, prosecutor Mark Lesko used Booth's false testimony about EXIF data as the basis for his argument that the alleged contraband photos were taken in 2005: "[EXIF] data is

[3] I base this finding on 1) the fact that CF card files were altered, 2) the motive for adding new files (to support the relationship between the CF card and WD HDD), and 3) the opportunity for alteration (the CF card was outside of Evidence Control for several months). This finding could be significantly strengthened (or disputed) if I were to be given access to both forensic copies of the CF card created on 04/11/2019 and 06/11/2019.

[4] The aforementioned DOJ/OIG report (https://oig.justice.gov/sites/default/files/reports/21-093.pdf), p.13 states digital evidence "must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious change."

[5] *Ibid*, p.83 "Moreover, the FBI Offense Code subjects FBI employees to discipline if they fail to "properly seize, identify, package, inventory, verify, record, document, control, store, secure, or safeguard documents or property under the care, custody, or control of the government."

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 which is consistent with the title of the folder." (p. 5571).

- **FE Booth minimized his knowledge about the previous CF card examination.** On page 4987 of the court transcript FE Booth acknowledged that the government had asked him to create "another report," meaning *in addition to the one created by FE Steven Flatley*. Therefore FE Booth knew, at a minimum, that FE Flatley had conducted an inventory of the camera and CF card, created a forensic copy the CF card, examined it with FTK (AD LAB), and then used FTK to create a report. However, when asked about his knowledge of what FE Flatley had done with the camera and CF card, FE Booth responded, "All I know is that he received it on that date. I have no idea exactly what he's done on the camera" (p. 4988).
- **FE Booth failed to disclose that his actions constituted a prohibited re-examination of digital evidence.** According to FE Booth's notes (DX 961), on 06/07/2019 SA Lever requested that FE Booth "process" item 1B15 (the Camera and the CF card) because FE Flatley "would be overseas during trial."
    - However, according to the Chain of Custody (DX 945) FE Flatley relinquished custody of the CF card to SA McGinnis on this same day (06/07/2019), so he was not yet "overseas."
    - FE Flatley was available to testify to his examination of the CF card, to include the forensic report he generated on 04/11/2019, *at any time during the preceding four weeks of trial*, which began on 05/07/2019. There was no legitimate need to re-examine the CF card and create a second report.
    - If FE Flatley was available to relinquish custody of the physical CF card on 06/07/2019, then he was also available to provide FE Booth with the forensic copy of the CF card he created (and named **NYC024299.001)**. FE Booth should have used the *existing* forensic copy to generate a new report, if needed, rather than creating his own forensic copy.
    - By creating a new forensic copy of the CF card (named **NYC024299_1B15a.E01**), FE conducted **a "re-examination" –** a duplication of all the technical steps that FE Flatley had already completed. CART policy strictly prohibits such re-examinations, unless approved by the executive management of the FBI Operational Technology Division.[6] I could not find a record of such an approval.

[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.

- Instead, according to his notes FE Booth only obtained approval from his acting supervisor Trenton Schmatz to proceed with the re-examination. Given the above facts, therefore, it is not credible that FE Booth had no knowledge of the fact that FE Flatley had already inventoried the camera and CF card, imaged and processed the CF card, and created an FTK report (GX 521A), especially when the government asked FE Booth to create "another report" (GX 521A "replacement"). Also it is not credible that FE Booth did not know his actions violated FBI policy on re-examinations.

- **FE Booth's testimony is especially troubling considering his status as a Senior Forensic Examiner.** In the FBI CART Program, an examiner may apply to be a senior examiner, which requires additional training, additional testing, a research project, and a special moot court exercise. As a Senior Forensic Examiner, Brian Booth should have known his actions were inconsistent with FBI CART policy and his testimony was false and misleading.

**Finding 6: The timeline of examination is suspicious.**

- 11 months passed between the seizure of the CF card (03/27/2018) and the date it was first delivered to a CART examiner (2/22/2019). As stated previously, several FBI employees – who were not authorized to view unexamined digital evidence – gained physical control of the CF card during that time. FE Flatley was the first CART examiner to receive the CF card and he imaged, then created an FTK report and file listing of the CF card on 04/11/2019. FE Booth first examined the CF card, from which the alleged contraband purportedly came, the day before he took the stand on 6/12/2019 - which was already more than four weeks after the trial began on 5/7/2019.
- It is highly unusual that digital evidence in such a case would be examined for the first time, by the testifying examiner, on the eve of his testimony. In my 20 years of FBI experience I have never seen such a delay – followed by a last-minute examination – in a case with no exigent (emergency) circumstances.

**Finding 7: Critical evidence was withheld from the defense team.**

- Examination photographs, including those documenting the initial condition of the evidence, were initially withheld (p. 4894). These photographs would include those taken of the evidence by FET Donnelly, FE Flatley, and FE Booth when they received them (on 08/08/2018, 02/22/2019, and 06/10/2019, respectively). In the examination notes of FET Donnelly and FE Booth, the examiners only included photographs of the WD HDD (1B16) and a Lacie HDD (1B28). Conspicuously missing were any photographs of the Camera (1B15) and CF Card (1B15a), as such photographs would document whether or not the evidence packaging was sealed when received by the examiner. Although FE Booth omitted the sealed status of the evidence in his notes, he admitted under oath that

the packaging for neither the camera nor the CF card was sealed when he received them (p. 4886-9).

- When a discovery order is issued by a court, it usually includes documents such as examination notes, reports, file listings, photographs, chains of custody, forensic images, and imaging logs. I have not seen a record of the government providing the CF card forensic image file (or forensic copy) created by FE Flatley (**NYC024299.001**), the CF card forensic image file created by FE Booth (**NYC024299_1B15a.E01**), or any of the logs and .CSV file listings that normally accompany the images. To my knowledge, no one has represented that alleged contraband exists on these forensic images and administrative documents, so there is no reason to withhold them from defense counsel. In **Appendix B** I have listed several of these evidentiary and administrative items that would be crucial to supporting my analysis but were not produced by the government before trial.

**Conclusion**

Never in my 20 years with the FBI have I seen a case brought to trial with such careless evidence handling, scant documentation, and obvious signs of evidence manipulation (see my Technical Findings report). The points above combined with technical findings of evidence alterations point strongly to the government, at a minimum, being aware that the evidence was unreliable and had been altered.

The government not only withheld this information from the jury but attempted to convey the opposite – that the evidence was reliable and authentic – by eliciting false testimony from FE Booth and making false and misleading statements in their closing arguments.

Respectfully Submitted,

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

# 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).

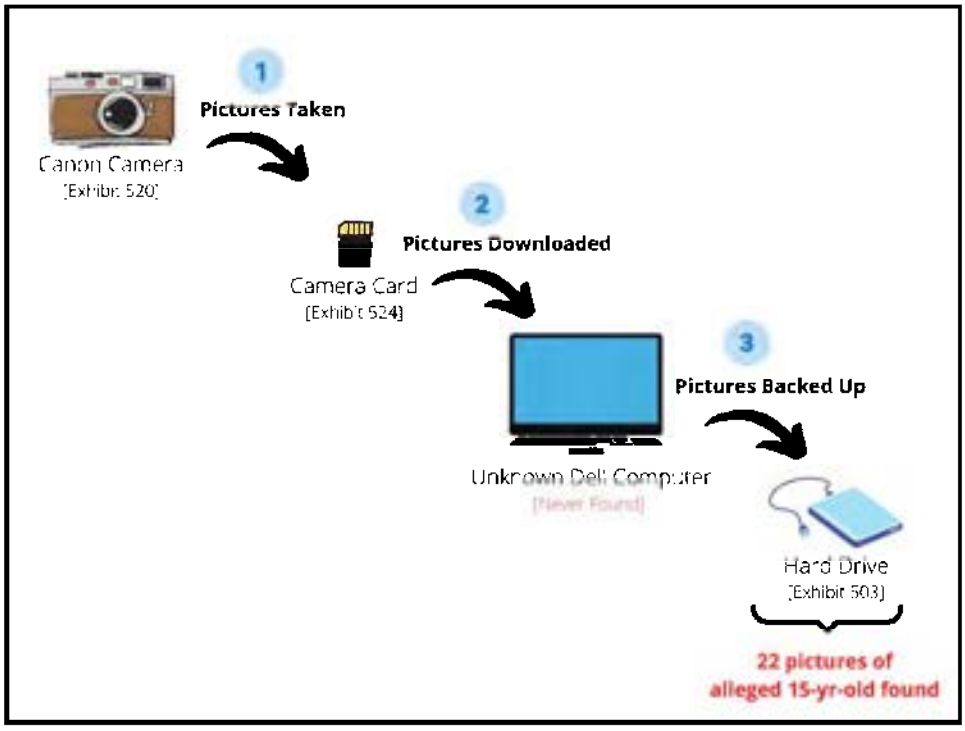



**Figure 1: The Government's narrative regarding alleged contraband found on a "backup" drive.**

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.

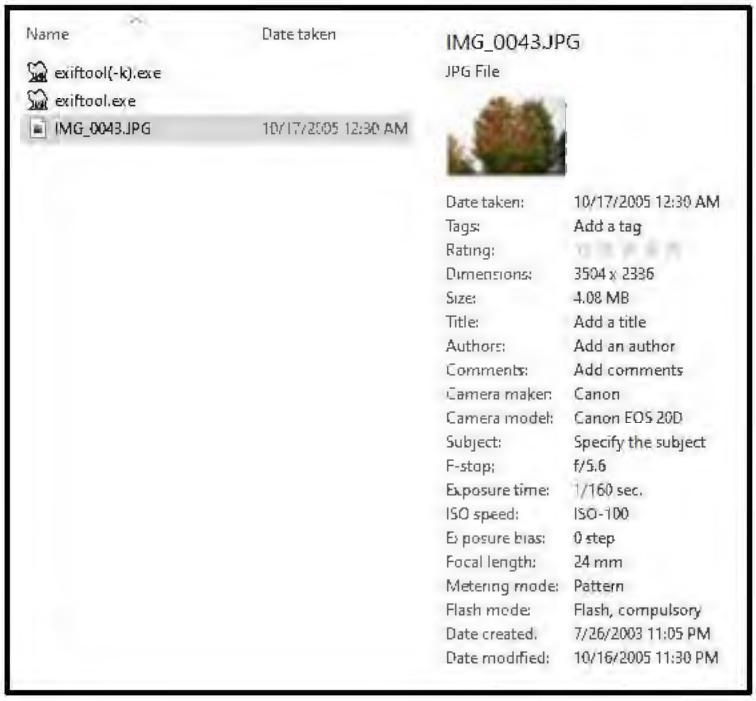


Figure 2. Windows display of EXIF data for IMG_0043.JPG.

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.

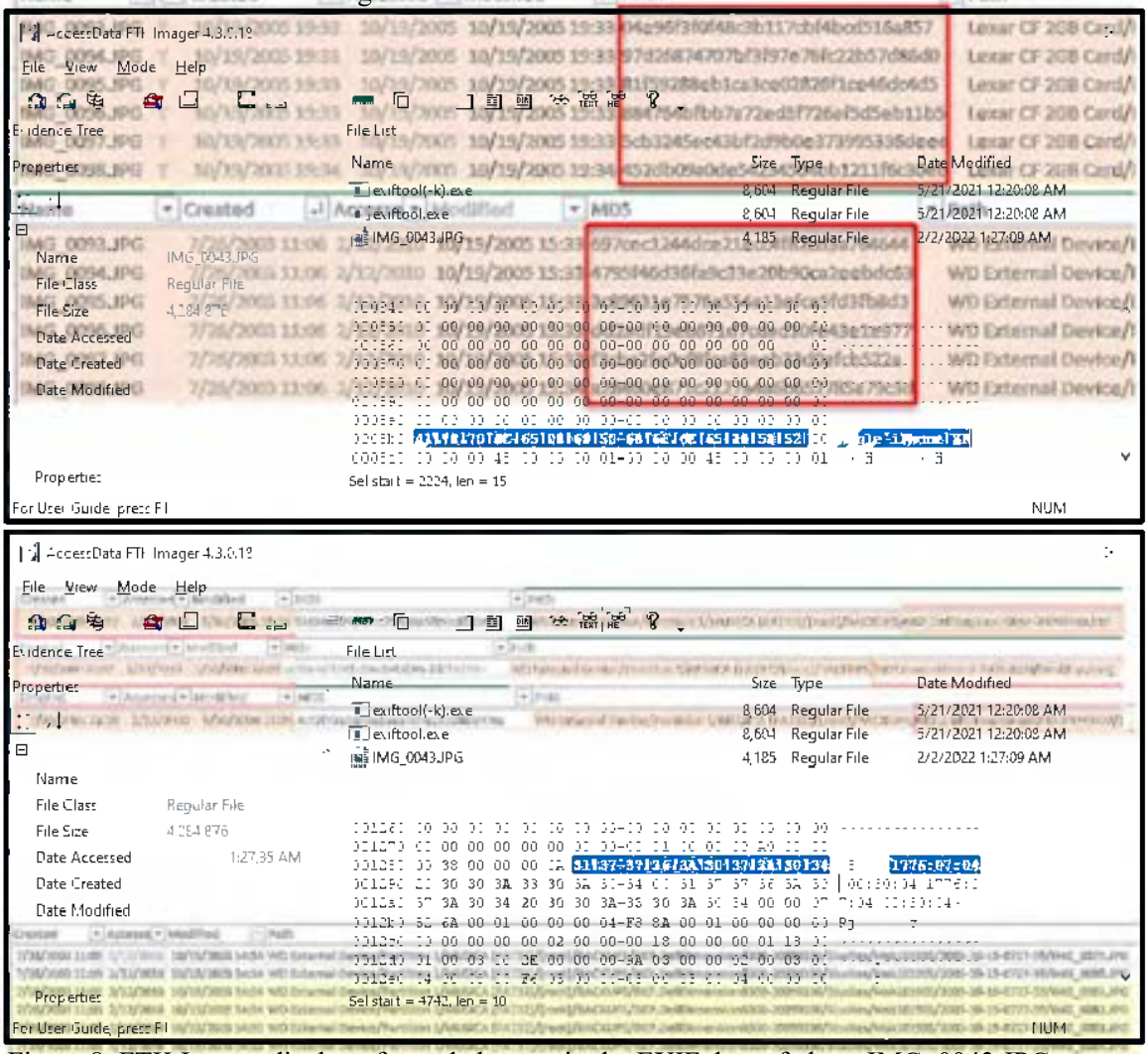



Figure 8. FTK Imager display of saved changes in the EXIF data of photo IMG_0043.JPG.

## Conclusion

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

I could have used one of the many freely available tools to modify the EXIF data that the **government claimed was "extremely reliable" "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.

# Appendix B

### Items Requested for Discovery

The following list represents critical evidence and administrative documentation that was not provided to me during my analysis of information pertaining to the case U.S. vs KEITH RANIERE, et al. After serving 20 years as an FBI Special Agent and Digital Forensic Examiner, I know these items should be readily available for the FBI to locate and produce in a timely manner, because most of these items are retrievable from the FBI Sentinel case management system or from the Evidence Control Unit (ECU), which is required to retain evidence for a criminal case until all appeals are exhausted. These items are critical to supporting my analysis of both the digital evidence and FBI procedures in this case, and to my knowledge none of these items were produced by the government before trial.

1. **The forensic image of the CF card (1B15a) created by FE Flatley (NYC024299.001)**, together with its imaging log and file listing (.CSV) file. This is a bit-for-bit duplication of the CF card, and I need to analyze it independently rather than rely on the FBI's submitted forensic reports. If the FBI did not delete it, this forensic image is located on the FBI shared server at: \\nycart-fs\cases05\NY-2233091_208206\Evidence\NYC024299\NYC024299.001. An archive copy should also be stored in the ECU.
2. **The forensic image of the CF card (1B15a) created by FE Booth (NYC024299_1B15a.E01),** together with its imaging log and file listing (.CSV) file. Again, I need to analyze this data independently from the FBI's forensic report, which shows new files were added to the 06/11/2019 report that did not appear on the 04/11/2019 report. My analysis of these two forensic images would determine to a scientific certainty which contents of the CF card were altered while in the custody of the FBI. If the FBI did not delete it, this forensic image is located on the FBI shared server at: \\nycart-fs\CASES02\NY-2233091_196817\Evidence\NYC024299_1B15a\NYC024299_1B15a.E01. An archive copy should also be stored in the ECU.
3. **FE Steven Flatley's complete Examination Notes.** These documents should include the steps taken by FE Flatley during his inventory, imaging, and analysis of the CF card, including software generated log files.
4. **Photographs of the CF card, documenting its condition and packaging, when received by FE Flatley on 02/22/2019 and by FE Booth on 06/10/2019.** FE Booth already testified he received the CF card in an unsealed plastic bag from the case agent. We have no information regarding the condition of the CF card when FE Flatley accepted custody of it.

5. **The original file listing of the WD HDD (1B16) created by FET Donnelly (NYC023721_1B16.E01.csv)** and the imaging log for that item. I need to compare the original file listing to that which was provided to me.
6. **The FTK log (generated by AD LAB) of the processing, browsing, searching, and bookmarking of digital evidence.** I need the FTK logs for the examination of the WD HDD (1B16) and both instances of processing for the CF card (1B15a). Among other important data, the FTK log would capture the date and time SA Lever allegedly "discovered" contraband on the WD HDD.
7. **The CART Requests corresponding to SubID 196817 and SubID 208206**. These documents are normally part of an examiner's "administrative notes," and could help explain the rationale for originally assigning the CF card to FE Flatley while assigning all the digital evidence items (including a reexamination of the CF card) to FE Booth.
8. **All EXIF data for ALL photographs listed on both of the CF card reports** (GX 521A, dated 04/11/2019, and GX 521A Replacement, dated 06/11/2019). I need to compare EXIF data contained in files contained in the forensic images of the CF card with those contained in the WD HDD files. However, if I am provided both forensic images of the CF card (Items 1 and 2) then I do not require this item.
9. **A detailed description (Examination notes) of how GX 504B was generated**, including the tool, options selected, and steps taken. Detailed examination notes are required to be able to replicate the results of the FBI's examinations.
10. **All communications**, including but not limited to texts, e-mail messages, notes, and voicemail messages, of FET Donnelly, FE Booth, FE Flatley, SA Lever, SA Jeffrey, SA Mills, SA Rees, SA McGinnis, AUSA Hajjar, and AUSA Penza, regarding this case. Among the above requested items, this is the only request for information that may not be readily retrieved from the electronic case file or from ECU. However, the communications between these DOJ employees would provide critical context to the actions taken regarding the collection, transportation, storage, and analysis of the digital evidence in this case.

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

# Analysis of the Testimony of Special Agent Christopher Mills

## 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 (See attached CV). 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

On March 27th, 2018, the FBI executed a federal search warrant at a two-story town home located at 8 Hale Drive, Halfmoon, New York. To my knowledge, the residence had been used as an executive library by Keith Raniere, defendant in the case U.S. vs KEITH RANIERE, et al. As part of my analysis of the digital evidence in this case, as well as the actions taken by the FBI to identify, collect, preserve, and analyze that evidence, I reviewed the testimony of FBI Special Agent Christopher Mills as he answered questions from prosecutor Tanya Hajjar regarding the search.

Among the many curiosities in this testimony, I was particularly struck by the fact that the first two pieces of evidence collected at the residence happened to be the ONLY two pieces of digital evidence used to convict Raniere of child exploitation. It was as if the FBI agents knew what would eventually be "found" on those devices and used at trial.

Moreover, in my opinion the questions by prosecutor Hajjar and the answers by SA Mills seemed specifically choreographed to give the jury the impression that the FBI followed robust procedures during the search, thereby distracting from the subsequent and obvious mishandling of the collected evidence.

**Testimonial Analysis**

What follows are referenced excerpts from SA Mills' sworn testimony, followed by my analysis regarding their significance to the case.

**1. Disproportionate attention to detail regarding search procedures rather than establishing an unbroken chain of custody.**

Prosecutor Tanya Hajjar asked, *"Agent Mills, can you just generally describe to the jury what the process is for conducting the search of a residence?" (p. 4290).*

What follows this quote was an unusually long and detailed description of FBI *search procedures*, complete with a discussion of the "knock-and-announce," forced entry, safety sweep, furniture present, search sketch, assignment of letters to each area, movement of agents through the residence, photograph procedures, etc. These 14 pages of detail stand in stark contrast to the vague, one-paragraph description of the *evidence collection and transportation* procedures recorded on page 4307 (discussed in #6, below). For example, the prosecutor introduced the search sketch, the photo log, and all the photos into evidence, but never introduced or even asked about the chains of custody or storage requirements for the evidence that was collected. From a reading of the transcript, it seems the over-emphasis on FBI search procedures was meant to distract from the under-emphasis on evidence handling procedures, which Hajjar must have known was problematic.

**2. A new agent, rather than the on-scene case agent, was the sole witness to testify about the execution of the search warrant.**

When asked about the search team, Mills answered: *"There was a team, mostly comprised of agents from the New York office, as well as the Albany office" (p. 4291).*

Despite the involvement of a sizeable search team from two different field offices, SA Mills (with only three years on the job) was the *only witness* asked to testify about how the evidence was identified and collected that day. His role was to "assist with evidence collection and documentation" and to take photographs. By contrast, SA Michael Lever, who was the lead FBI investigator in the case (the "case agent"), the affiant on the search warrant, and was probably responsible for the mishandling of the digital evidence for many months after the search[1], did NOT testify during the entire trial. A reasonable person may conclude that the prosecutor intentionally limited the risk of exposing the FBI's evidence mishandling by declining to put the case agent on the stand.

[1] See my Technical Findings and Process Findings reports.

**3. The search team ignored several other areas of the residence before starting to search the office.**

Hajjir asked, *"And where did you go from there, in terms of initiating the search?" (p. 4294).*

During the unusually long description of the movements of the search team, Mills indicated they moved past the kitchen, living room, bathroom, and open areas of the first floor. Then they took a spiral staircase to the second floor, where they moved through several more areas, including a bathroom, and a seating room area, before finally arriving at the "office space." Although the office was the last of many areas discovered in the residence, it became the first area to be searched. In my experience, the case agent normally assigns groups of FBI personnel to search different areas of the building simultaneously to save time. Working this way in multiple simultaneous locations, search teams would be able to collect evidence, but no one would be able to assign consecutive evidence numbers. In this case, however, someone decided the office would be the first location to start finding AND numbering evidence.

**4. The very first item to be identified in the entire residence was a camera with a camera card, located under a desk, and which happened to be one of two key pieces of digital evidence used to convict Raniere of child exploitation.**

In describing one of the search photographs he took, SA Mills said, *"So the there's a note there with the number one. So number one represents evidence item number one. So, in this case, this photo was taken underneath the desk or table and was assigned number one based on being the first evidence item that was found" (p. 4304).*

If SA Mills' account is correct, then the FBI search team traversed several areas of the residence, went upstairs and straight to the office area, and then crawled under a desk to find the first piece of evidence – a camera bag containing a camera and camera card. At this point, the case agent, SA Lever, had not yet "discovered" alleged child pornography taken with this camera, so it seems more than a strange coincidence that it was the first evidence item identified.

Another anomaly is the fact that an item number was assigned to the camera immediately upon discovery. All the items documented in the photo log (GX 502) and represented in the photographs (GX 502A) have item numbers, written on sticky notes photographed next to the items. Generally, FBI search personnel do not assign item numbers to evidence at the moment of discovery/photography/collection, because there are multiple people working in different rooms and it would be impossible to coordinate the numbering among them. If any items are assigned item numbers, then it is done near the *end* of the search when the seizing agent collects all the evidence together and fills out the FD-597 receipt for items seized. Therefore, in practice the item numbers rarely correspond to the order in which they were collected.

**5. The very next item to be identified in the entire residence was an external hard drive, located away from the desk on a shelf, and which happened to be the second of two key pieces of digital evidence used to convict Raniere of child exploitation.**

When asked about another photograph he took, SA Mills answered, *"So this is the still of the same office space as seen before and item number two, which is on top of the bookshelf here, is a gray or silver hard drive" (p. 4308).*

Once again, it is extremely convenient that from all the potential evidence in the residence, it was the Western Digital hard drive – where the alleged child pornography was stored – that was the *second* piece of evidence identified by the FBI on scene. It is also important to note that the camera card (Item #1) and the hard drive (Item #2), comprised the entirety of the child exploitation digital evidence against Raniere – which supposedly was not "discovered" by the FBI for nearly a year later.

**6. Prosecutor Hajjar did not even attempt to establish an unbroken chain of custody for the digital evidence used against Raniere.**

Hajjar: *What happens when you recover a piece of digital evidence like Government Exhibit 520 and 524?*

Mills: *So, when we receive -- when we recover digital evidence, we have a process in which we bring the digital evidence back to our office and if we want the evidence to be reviewed, we would submit a request to our CART team. And the CART is the Computer Analysis Response Team and they have specialists who are computer evidence examiners who would review that evidence for us or assisted us in reviewing the evidence with us.*

Hajjar: *And is that what happened in this case with Government Exhibit 520?*

Mills: *Yes.* (p. 4307).

After spending several minutes eliciting the details of search activities, the prosecutor was strangely disinterested in establishing an unbroken chain of custody for the two pieces of digital evidence presented at trial. Conspicuously missing were the following questions, for example:

- Who decided which pieces of evidence were relevant and within the scope of the search warrant?
- Why did you bypass documents and other potential evidence in other rooms in order to start with items in the office?

- While in the office, why did you start identifying and collecting evidence beneath the desk?
- The photo log shows that you went back and forth from room to room, photographing various evidence items there. Why didn't you stay in one room to photograph all the evidence there, before moving on to the next room?
- Who decided the order in which the items were to be photographed and assigned item numbers?
- After you photographed each piece of evidence, what specifically did you do with it?
- Who sealed the evidence?
- Who packaged the evidence?
- Who started the chains of custody for the evidence?
- Who transported the evidence back to your office?
- Who took custody of the evidence at the office, and how was it stored?
- You said you found the camera card (CF card) inside the camera (p. 4305). You must have removed it on scene to identify it here in court. Who removed it permanently and put it inside a cellophane bag?
- Why didn't you photograph the CF card after you discovered it inside the camera?
- Why wasn't the CF card noted on the photo log, chain of custody, electronic evidence entry, or any other documentation related to the seizure of the camera?
- When was this evidence relinquished to case agent Michael Lever?
- How long did he have custody of the evidence?
- Did you realize that the camera and the CF card were in unsealed containers when you regained custody and relinquished them to FE Booth on 06/10/2019?
- Who unsealed them and why were they not re-sealed?

In the above trial excerpt, it seems the prosecutor specifically crafted her sentence to avoid discussing *who* in the FBI had taken actions on the digital evidence after it was identified at the search site. As I detail in my Process Findings report, the chains of custody demonstrate that SA Lever and other FBI individuals not authorized to review unexamined digital evidence gained physical control over the digital evidence for several months before turning it over to CART forensic examiners. In fact, the CF card was checked in and out of the Evidence Control Unit (ECU) for eleven months before it was finally released to the first CART examiner, Stephen Flatley, on 02/22/2019. During that time, as the government has acknowledged, an FBI employee accessed that camera card on 09/19/2018. The Chain of Custody indicates that the case agent, SA Michael Lever, had custody of the CF card from 09/19/2018 to 09/26/2018. In my Technical Findings report, I describe several anomalies that demonstrate manual manipulation of data on that card.

The Chain of Custody also shows that other FBI employees, SA Elliot McGinnis and SA Christopher Mills, regained custody of the camera and CF card from the first CART examiner

before turning it over to a second CART examiner, Brian Booth, in *unsealed packaging* on 06/10/2019 – *the very day Mills testified about collecting it*. As explained in my Process Findings report, a second examination of digital evidence is strictly prohibited by policy, and for the second examiner to receive the original evidence from a case agent (rather than using the work of the previous examiner) is very abnormal.

Regarding SA Lever's handling of the digital evidence in this case, there are several questions that must be answered, for example:

- Why did SA Lever and other FBI employees check out the evidence from the ECU multiple times, when they were not authorized to even look at it?
- Why did SA Lever access the CF card without a write blocker on 09/19/2018?
- Why does the Chain of Custody for the WD HDD (DX 960) end with SA Lever checking it out of Evidence Control on 02/22/2019?
- What did SA Lever do with the WD HDD after he checked it out?

It is very telling that the prosecutor completely avoided the topic of chain of custody with respect to the digital evidence in this case.

**7. Sometime after collecting the first and only two pieces of digital evidence eventually used at trial, the searching agents returned to the space beneath the desk and collected another external hard drive.**

After being asked to describe another photograph he took, SA Mills said, *"So this is, once again, underneath the desk or the table in the office space. And you see item number 14, so that's evidence item number 14, the gray or silver hard drive" (p. 4310).*

SA Mills later identified this second external hard drive as a LaCie external hard drive (Item #14). If (according to SA Mills) the item numbers correspond to the order in which they were collected, then this item was *discovered in the same place as the camera bag* (Item #1) – yet it was not discovered and collected until much later. In fact, according to the seized property receipt[2] and the search photos (GX 502A), the FBI collected a book, 30 cassettes, an Amazon Kindle, two CD discs, a thumb drive, and miscellaneous documents before returning to the space beneath the office desk to collect the LaCie hard drive and other computer equipment.

This strange behavior begs the following question: Why did the FBI agents first go straight to the camera bag (Item #1), located under the desk, then search a shelf, where they retrieved an external hard drive (Item #2), then collect dozens of other items (some found in other rooms) before returning under the desk, where they found the LaCie external hard drive?

[2] See FD-597, Receipt for Property Seized.

**Conclusion**

The prioritized collection of the only two pieces of digital evidence used to support the child exploitation charges at trial (Items #1 and #2) strongly points to foreknowledge on the part of the FBI agents. In fact, a reasonable person would suspect the evidence collection process itself was influenced **by someone with an interest in the FBI "finding"** digital evidence against Raniere.

Moreover, the question-and-answer interactions between prosecutor Hajjar and SA Mills seemed intent on convincing the jury of the reliability of the digital evidence through a robust discussion of FBI *search* procedures, while deliberately obfuscating the **FBI's** *aberrant evidence handling* activities that occurred thereafter. In short, the testimonial evidence recorded in this court transcript is consistent with the evidence manipulation opinions and conclusions expressed in my Technical Findings and Process Findings reports.

Respectfully Submitted,

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

**J. Richard Kiper, PhD, PMP**

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

# Expert Opinion Regarding Time to Review Digital Evidence

## 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 (See attached CV). 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.

## Review of Events

In my experience serving in the FBI's Computer Analysis Response Team (CART), forensic examiners are typically given several months to examine digital evidence and prepare analyses for legal proceedings. Similarly, a court's discovery order usually requires that evidence against the accused be provided to the defense team with enough time to prepare a reasonable defense. In the case of U.S. vs KEITH RANIERE, neither of these norms were followed.

Two digital devices – a camera card (CF card) and an external hard drive (WD HDD) – were the only pieces of digital evidence used to support the government's charge of child exploitation in this case. However, despite having possession of these items for a year, the FBI did not provide defense counsel any access until 03/13/2019[1], a mere twenty-six days before jury selection was scheduled. At that time, the FBI gave the defense access to the forensic image of the *external hard drive only*, and due to the allegation of child pornography, the defense expert could not remove any data from the premises beyond screen shots of file listings and handwritten notes.

Further impeding the ability of the defense to conduct a thorough review of the evidence with its own forensic tools, the FBI did not provide a "clean" (non-forensic) copy of the contents of the hard drive until 04/06/2019, less than a week prior to the scheduled jury selection.

[1] This was also the date of the government's Second Superseding Indictment alleging sexual exploitation of a child. According to the FBI examiner's notes, 03/13/2019 was the date the hard drive image was prepared for review. I do not know when the defense expert was provided access to review it.

Finally, the FBI significantly delayed the creation and delivery of the forensic reports used at trial. According to the sworn declaration of defense counsel Marc Agnifilo filed on 04/22/2019, "…when asked recently when we were going to get these reports, the prosecution stated that the reports were not completed but that the government would make the reports available when the FBI completed them." In fact, the "not completed" forensic reports already had been completed on 04/11/2011 but *were still being withheld from the defense team two weeks prior to opening statements*.

The government's delay of the second forensic report of the CF card was even more egregious. The FBI first examined the CF card and created a forensic report on 04/11/2019. Then, more than four weeks AFTER trial had begun – and against FBI digital evidence policy – the FBI conducted a *second examination* of the CF card[2] resulting in a *second forensic image* and generated a "replacement" report of the CF card on 06/11/2019. The defense team literally had no time to prepare a technical rebuttal before this report was introduced at trial.

**Required Analysis**

A defendant is entitled to the opportunity to review, analyze, and rebut the evidence used against him. At a minimum, the analysis of digital evidence in this case should have included the following tasks:

- A review of the legal authority to conduct the examination.
- A review of the evidence collection, packaging, transportation, and storage procedures.
- A review of the chain(s) of custody.
- A review of the examination notes and administrative paperwork.
- Verification of evidence integrity (e.g., via MD5 hashing).
- Reproduction of the forensic steps used to produce the alleged results.
- New analysis of evidence, including but not limited to:
    - File system metadata,
    - EXIF data,
    - File content,
    - Application artifacts,
    - Operating system artifacts, and
    - Timeline analysis
- Creation of new trial exhibits to rebut the government's narrative.

In my expert opinion, it would be impossible for a defense expert to have completed the above listed activities within a mere twenty-six days (in the case of the hard drive) much less instantaneously (in the case of the CF card).

[2] See my Technical Findings and Process Findings reports, where I describe this anomaly in detail.

**Conclusion**

The government placed the Raniere defense team at a significant and unjust disadvantage by intentionally withholding key evidence they intended to use at trial. At best, the defense team was given only twenty-six days to conduct a technical review of *some* of the digital evidence (a non-forensic and partial copy of the hard drive contents) and at worst, it was given *no opportunity* to review the second FTK forensic report related to the CF card.

It is my expert opinion that it was unreasonable to expect the defense team to have conducted a forensic analysis of the digital evidence in this case within the given time frames.

Respectfully Submitted,

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