Summary of the Technical Findings of Digital Falsification in *US v. Raniere*
November 27, 2024

By:
Dr. James Richard Kiper, Ph.D., Retired FBI Special Agent and Forensic Examiner
Stacy Eldridge, Former FBI Senior Forensic Examiner
Mark Bowling, Retired OIG and FBI Special Agent and Forensic Examiner
William Odom, Former FBI Special Agent and Forensic Examiner
Steven Abrams, Digital Forensics Examiner
Stephen Bunting, Digital Forensics Examiner
Wayne Norris, Digital Forensics Examiner

I. Introduction

Our joint analysis revealed that a camera's memory card and a hard drive – key evidence of charges "at the heart" of the government's racketeering case – were extensively falsified.[1] This report reviews the 11 technical findings of digital falsification, examines their current status, and further details two of the findings regarding the memory card. As outlined, **none of these findings have been scientifically refuted.**

II. Case Background

The camera, its memory card, and the hard drive were pivotal to the government's case, forming the basis of the child pornography and sexual exploitation charges. The government alleged that the defendant used the camera to photograph a 15-year-old, saving the photos to its memory card before transferring them to an unlocated Dell computer and later backing them up to the hard drive. The Government claimed these photos were taken in 2005.

Notably, the photos were not argued to be visually obvious as contraband. The photographed subject did not testify. Their age of 15 was inferred from the photos' metadata (EXIF data)—information embedded in the files that indicate when the photo was taken, but is easily manipulated[2]. (Trial T. (6/12/19) at 4817:18-4818:20). The metadata indicated that a series of photos, including the alleged contraband, were taken by the camera in 2005.

It is vital to explain the notion of metadata. Metadata is "data about data". For example, the words of a book are its data, and the title page [including the data of publication] and the numbers at the bottom of each page are its metadata. If the book is placed into a library, the date of publication is also found in the library's filing system.

---

[1] *See US v. Keith Raniere et al.*, EDNY, 18-cr-204, Doc. 1253-1, hereinafter referred to as "Joint Report"
[2] *See* Dr. Kiper's Report, Doc. 1169-1 at PageID #21389-21396

Unlike books, files cannot exist in isolation - they must be stored on a drive of some type. That is essentially like saying all books must be in a library, which is far-fetched for books, but the only possibility for data files.

If someone views a file in, for example, Windows Explorer, the file's observed date (be it created, accessed, or modified) is the date Windows reports from the file system, not the EXIF data for that file.

If someone views the same file in, for example, Adobe Bridge or "exiftool", the observed date (be it date/time original, create date, modify date, or others) is the date from the file's EXIF data, not the file system timestamps.

File system dates and EXIF dates are both forms of metadata and arise from different processes. They are also stored in different locations, the former in a file system component (the MFT in an NTFS format or in the directory entry in a FAT format) and the latter in the beginning of the file data itself. The correlations between these two types of dates - and in certain cases, the lack of correlations - are vital in this case.

While the memory card did not itself actually contain contraband, it included photo files that appeared to come from the same series that was located on the hard drive and were allegedly taken by the camera. Linking the photos on the hard drive to the camera was critical to the government's case, as it was used to tie the defendant to the photos' creation.[3]

III. Summary of Key Findings

- The alleged contraband and other photos on the hard drive were planted.[4]
- A report from the second forensic image of the memory card (a forensic image is an exact replica of the data) shows 37 additional photo files that were not in the report of the first forensic copy. Access to both forensic copies is needed to explain this critical discrepancy.[5] We identified 28 of the 37 additional photo files as being intentionally manipulated.[6]
- **(Uncontested by the government)** Dozens of photo files were planted on the memory card using a computer, and then their file system creation timestamps (indicating when they were added to the card) were each manually altered making it falsely appear as though the seized camera—not a computer—took and saved them in continuous batches in 2005, 2006, and 2007.[7]

[3] Trial T. (6/17/19) at 5372:17-5373:5
[4] *See* Joint Report, Technical Finding 7
[5] *See* Joint Report, Technical Finding 2
[6] *See* Joint Report, Technical Findings 8, 10, and 11, summarized in ¶ 15
[7] *See* Joint Report, Technical Findings 8 and 9

- **(Uncontested by the government)** Last accessed dates of dozens of photo files on the memory card were manually tampered with and set to dates in 2005[8].
- **(Uncontested by the government)** Folder names on the hard drive were altered, falsely suggesting the photos were downloaded on specific dates in 2005.[9]
- Timestamps of photo files on the hard drive were manually adjusted, "most plausibly … to mimic an automatic Daylight Savings Time change from 2005"[10], further falsely supporting the 2005 timeline.
- The EXIF timestamps of a non-contraband photo, within the same sequence as the alleged contraband, were deliberately altered, apparently to conceal that the file had been modified using Photoshop Adobe Elements.[11] However, a record of that alteration was left in the EXIF metadata, allowing us to discover it.

Additionally, the memory card was altered while in FBI custody before it was sent for forensic preservation —a fact admitted by the government during the trial. Over four years later, it was revealed that this alteration was caused by an unauthorized FBI photograph technician who was concealed from the chain of custody. Despite repeated requests, the government has refused to identify this individual.

The undersigned former FBI CART examiners previously concluded that these knowing violations of FBI protocol altogether are unprecedented in their combined 55 years of service to the FBI and lack any legitimate explanation.

IV. Detailed Discussion of Findings and Their Status

After the trial, the government enlisted FBI Senior Computer Scientist David Loveall II to respond to Dr. Kiper's technical findings.

However, Loveall's responses addressed only Dr. Kiper's conclusions and ignored additional observations submitted by other forensic examiners. These observations were submitted in the motions to which the government was opposing, using Loveall's responses..

Furthermore, neither the government nor Loveall contested the numerous FBI protocol violations uncovered by Dr. Kiper and Ms. Eldridge in the handling of this digital evidence. A summary of these protocol violations is provided in the table below:

[8] *See* Joint Report, Appendix A, Technical Findings 10 and 11
[9] *See* Joint Report, Technical Finding 6; see also Dr. Kiper's Report, Doc. 1169-1 at PageID # 21357-21358
[10] *See* Joint Report ¶ 9
[11] *See* Joint Report, Technical Finding 5, addressed in ¶ 10

Key <u>Uncontested</u> Process Findings	
Expert	Finding
Kiper	FBI Senior Forensic Examiner (SFE) Brian Booth, who testified about his analysis of the camera and memory card at trial, received this evidence **unsealed**, creating a broken chain of custody. (Doc. 1169-1 at PageID # 21382)
Kiper	Special Agents (SAs) Maegan Rees and Michael Lever each checked out from Evidence Control the camera, containing its unpreserved memory card, for review, without authorization, in violation of FBI protocol, with SA Rees holding it for 17 days and SA Lever for 7 days. (*Id.* at PageID #21383)
Kiper	SFE Booth knowingly gave false testimony, including the following points: 1. Receiving unsealed evidence is not extraordinary: In Dr. Kiper's 20 years in the FBI, he never received unsealed evidence, except in exigent circumstances, which did not exist here. (*Id.* at Page ID # 21382, 21385) 2. SFE Booth did not know who had the evidence prior to his examination, two days prior to his testimony. (*Id.* at Page ID # 21385). 3. SFE Booth repeatedly represented EXIF data as reliable (*Id.*). 4. SFE Booth minimized his knowledge about the previous memory card exam. (*Id.* at Page ID #21386).
Kiper	SFE Booth created a prohibited second forensic image of the memory card, in violation of FBI protocol, and Supervisory Special Agent Trenton Schmatz improperly approved it. (*Id.* at PageID #21386-21387).
Eldridge	The US Attorney's Office was provided the original, unpreserved memory card, which is prohibited by FBI protocol. (Doc. 1192 at PageID # 22022).
Eldridge	An unauthorized forensic exam was done on the unpreserved memory card in September 2018, outside of CART, which is prohibited by FBI policy. (Doc. 1192 at PageID # 22022).

Finally, Loveall did not respond to additional technical findings by the undersigned, which the government had an opportunity to respond to, as these findings were included in the defense's motion for reconsideration to compel the two forensic copies of the memory card. These findings are discussed in greater detail herein.

1. **The Alleged Contraband, and the Other Photos, Were <u>Planted</u> on the Hard Drive and Disguised as a Computer Backup (Contested)**

   a. **Our Finding (Technical Finding #7)**

The hard drive contained three folders, each appearing to result from an automatic backup on March 30, 2009. One folder, "BKP.DellDimension8300-20090330," was allegedly created by a Dell computer, which was not among the devices collected pursuant to the March

27, 2018 search warrant but claimed by the government to belong to the defendant. This folder's creation date, March 30, 2009, matched the folder name, supporting that an automatic backup occurred on that date. This folder contained the alleged contraband.

However, the files inside of the purported March 30, 2009 backup folder, including the alleged contraband, show a file creation date of July 26, 2003—six years before the backup and before the camera that supposedly created the photos existed. If the files were part of a genuine 2009 backup, their file creation dates would match the 2009 creation date of the folder.

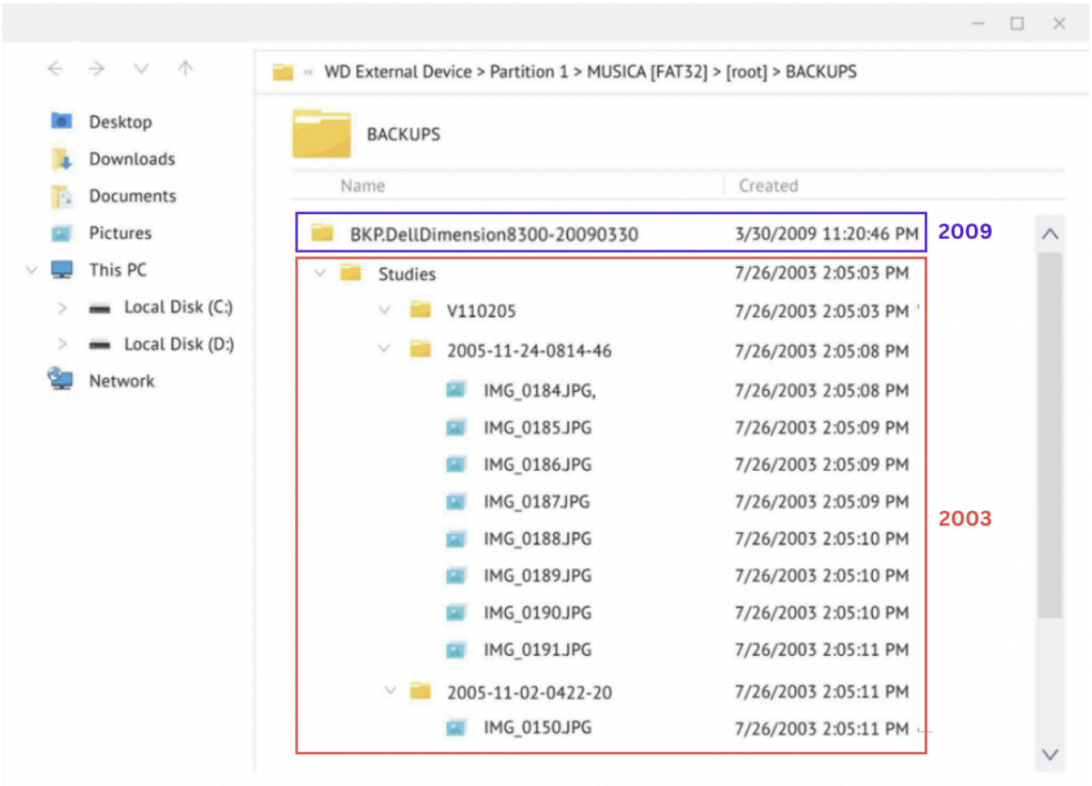
This mismatch is akin to finding a new sealed soda can labeled as Coca Cola but filled with lemonade. Soda canning is a fully automated process where the contents (cola) and the container (label) are expected to match perfectly. Similarly, in this case, the folder and its contents are expected to align because computer backups automatically assign file creation timestamps (file system) to files during the backup process. Such a discrepancy, the contradictory 2009 and 2003 file system timestamps, demonstrates evidence falsification. This discrepancy proves that the files were not from an automatic computer backup[12] but could only have been **manually** placed in the folder later and "disguised as a computer backup." A normal user would not do this.

This evidence of these actions constitute planting of the photos, invalidating the folder as a legitimate backup. **This directly undermines the government's possession charge, which required the photos to be authentically on that hard drive.** (Doc. 430 at 9, "the defendant … did knowingly and intentionally possess … [contraband] contained in digital files stored on a Western Digital hard drive.").

(The rest of this page intentionally left blank)

[12] There are additional anomalies with the backup folder, noted in our original reports, e.g. *see* Dr. Kiper's Report, Doc. 1169-1 at PageID# 21359-21360.

Diagram 1: Contradictory 2003 Dates in Alleged 2009 Backup Folder[13]



b. Evaluation of Loveall's Rebuttal

The government's expert, Loveall, failed to address the central issue of the anomaly: how files with 2003 file creation dates could appear in a folder from an automatic backup with a file creation date of 2009. His response focuses only on explaining the 2003 dates but ignores the critical contradiction with the backup folder's 2009 date.

Summary of Loveall's Response	**Critique of Loveall's Response**	**What a Proper Response Should Look Like**
Loveall claims that files dated 2003 could result from a clock reset on a "Dell Dimension 8300 with a bad battery." He tested a computer he referred to as "Dell Dimension 8300-20090330" and concluded the 2003 dates were consistent with such a clock reset.	**Ignores the Main Issue**: Loveall focuses on explaining 2003 file dates, but does not address how files with those dates could appear in a folder created in 2009. **Blatant Error**: He claims to have tested a "Dell Dimension 8300-20090330,"	A valid response would: 1. Use a Dell Dimension 8300 to replicate the setup. 2. Connect the same model of external hard drive used in the case, and formatted to a FAT-32 file system.

[13] This diagram was originally included in the Joint Report, Pg. 3 as Diagram 2.

(Doc. 1213-3, Loveall Report ¶¶ 17-18).	which is not a real computer model but a folder name. **Does Not Test the Issue**: He did not test whether an automatic backup in 2009 could produce files dated 2003 while creating a folder dated 2009, which is the anomaly.	3. Run automatic backup software consistent with what was available in 2009. 4. Reproduce the anomaly: files dated 2003 inside a folder created in 2009, through an automatic backup. 5. Document each step thoroughly, providing reproducible results and clear evidence.

As shown above, Loveall's response was scientifically invalid - it was speculation. Therefore, our finding stands: the alleged contraband was falsely planted on the hard drive.

2. 37 Additional Photo Files In the Report of the Second Forensic Copy of the Memory Card, Raising the Question of Planting in FBI Custody (Contested)

a. Our Finding (Technical Finding #2)

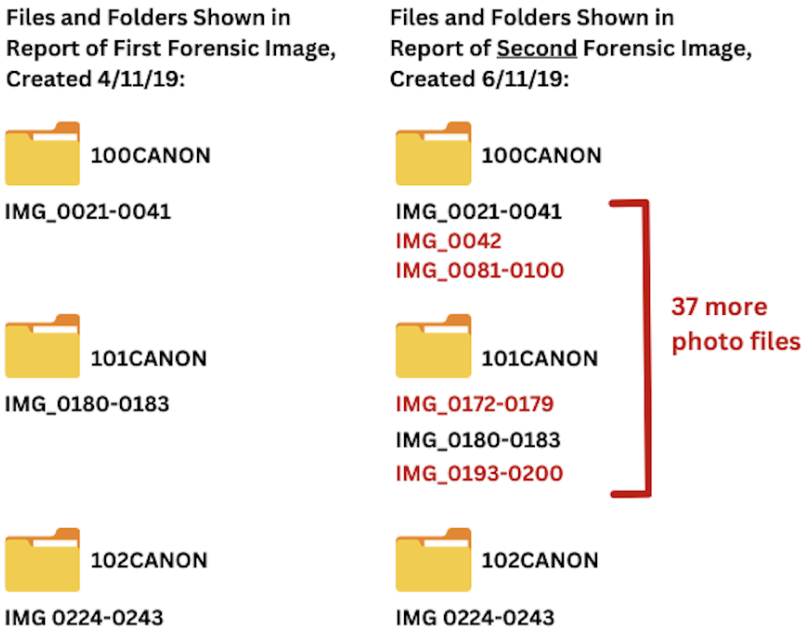
During the trial, on June 11, 2019, FBI examiner Brian Booth created a second forensic copy of the camera's memory card. FBI protocol allows only one forensic image to be created from the original device; any subsequent copies are to be made from that first forensic image.[14] This second copy was made months after the first one. To confirm that two copies are identical, hash values—a unique digital fingerprint—are used. However, the second copy was never produced, and hash values have not been provided to verify it matched the first. Production of hash values is so basic to computer forensics that most forensic software creates them automatically. **To not provide them is exceptional.**

The report from the second copy showed 37 more photo files than the first, all appearing in the same folders as the photo files from the report of the first copy.[15] This raises serious questions about when and how these files were added and whether this happened between the creation of the two forensic copies.

Notably, of these 37 files, we determined that 28 were intentionally manipulated (see Technical Findings #8 and #11, discussed below)**. The government has withheld access to both the first and the second forensic copies of the camera card**, preventing further analysis.

[14] *See* Dr. Kiper's Report, Doc. 1169-1 at Page ID# 21386
[15] *See* Dr. Kiper's Report, Doc. 1169-1, PageID# 21354-21355

Diagram 2: 37 Photo File Discrepancy Between the Reports of the Two Forensic Copies



b. Evaluation of Loveall's Rebuttal

Loveall's rebuttal contains critical errors, omissions, and unverified claims.

Summary of Loveall's Response	**Critique of Loveall's Response**	**What a Proper Response Should Look Like**
Loveall stated, "The fact that additional files appeared in one report is a result of the use of different settings. I have examined the disk images created of **1B15** and **1B15a** and determined that they are identical." (Loveall Report ¶ 9) (emphasis added).	**What is a "Disk Image"?**: A "disk image" is another term for a forensic copy, which contains the data extracted from a device. This is not the same as an "image" meaning a digital photo of the device. **Wrong Identifiers:** Loveall refers to 1B15 (camera) and 1B15a (memory card), but these are device identifiers, not the correct labels for the forensic copies (NYC024299.001 and NYC024299_1B15a.E01).	A valid response would: 1. Accurately reference the memory card forensic images (NYC024299.001 and NYC024299_1B15a.E01). 2. Verify data integrity by providing the hash values for both images, proving they are identical. 3. Provide a detailed explanation of the settings used for each report and demonstrate how they account for the 37 photo files appearing only on the report of the second forensic copy.

	So What Is He Saying?: The question was whether two forensic images of the same card are different. Loveall is answering a different question - one that was not asked. Loveall is literally claiming that the forensic copy of the camera (1B15) is "identical" to the forensic copy of the memory card (1B15a). This is impossible for two reasons: - **Impossibility 1:** Cameras like 1B15 (Canon EOS 20D) do not have internal storage, so it is impossible to create a forensic copy of the camera itself. - **Impossibility 2:** The camera and memory card are separate devices with different data. Their forensic copies would not be "identical," and this is not even the correct comparison. The proper comparison is between the two forensic copies of the memory card. **Errors Might Not Be Obvious:** These errors and impossibilities in his statement might not be obvious to a non-technical audience, but fundamentally undermine Loveall's claims. **Vague and Unsupported "Examination":** Loveall claims he "examined" the forensic copies, but provides no details on how he did this. He offers no hash values (unique digital fingerprints),	4. Fully document all steps taken, including screenshots or logs, to ensure transparency and reproducibility.

	needed to confirm the data's integrity. This is a basic and required practice in digital forensics.[16] **Settings Claim Lacks Proof:** Loveall speculates, without evidence, that the discrepancies are to "settings" differences, but does not specify what settings were used or provide any actual evidence whatsoever to support this claim.	

Loveall's response is scientifically invalid. speculative, and unsupported. It fails to establish that the forensic copies are identical, leaving the question as to whether the 37 photo files were planted in FBI custody between the creation of the two forensic copies unanswered. This is a question that could easily be resolved if access to the second forensic copy were granted to the defense – access that was exclusively given to Loveall post-trial to form his report. Access to the two forensic images would also likely lead to additional proof of falsification, because having the full data allows for a more comprehensive analysis.

3. Planting of Photo Files on the Memory Card and Manipulation of File System Timestamps, Using a Computer, Mimicking Real-Time Camera Capture (Uncontested)

a. Background About the Camera and File System Timestamps

When this camera takes photos, it saves them to the memory card. At that point in time, for each photo, the camera generates several timestamps, including:

- a **file creation timestamp in the card's File Allocation Table [FAT],** reflecting when the photo file was saved to the card, and
- an **EXIF timestamp inside the file itself,** reflecting when the photo was captured

[16] Loveall's failure to perform a basic verification of the two forensic images by comparing hash values is problematic, given that it is a standard procedure in digital forensics, and that the hash values would have definitively confirmed his claim. Notably, the government has offered Loveall in another case as an expert in the exact topic of verification through hash values (See the government's notice of expert testimony in *USA v. Trump* (Southern District of Florida), 23-cr-80101, Doc. 257-6). The notice states that Loveall "has not testified as an expert in a trial or by deposition in the last four years" except for in this case. (*Id.* at 2).

To reiterate, the file creation time is saved to the memory card's **file system**, which is like a table of contents that keeps track of where and when files are saved on the card. The EXIF timestamp is saved inside the photo file, like a note written directly on the photo itself.

When photos are moved to a computer or backed up to a hard drive, the EXIF timestamp remains unchanged, but the file creation timestamps of the transferred photos, e.g. on the hard drive or computer, would have an updated file creation timestamp, reflecting the date and time of transfer. This is illustrated in the diagram below.

Diagram 3: Illustrating the Automatic Behavior of File Creation (File System) and EXIF Timestamps Upon Transfer (Hypothetical Example)

*Original Photo File on the Memory Card, taken at **01/01/2008 11:11:10 PM***

File Name	File Creation Timestamp	EXIF Timestamp
IMG_300	01/01/2008 11:11:10 PM	01/01/2008 11:11:10 PM

*Photo File on the Computer, After Transfer from the Memory Card on: **6/6/2008 at 2:00:00 PM**.*

File Name	File Creation Timestamp	EXIF Timestamp
IMG_300	**6/6/2008 2:00:00 PM (changed)**	01/01/2008 11:11:10 PM (unchanged)

*Photo File on the Hard Drive, After Transfer from the Computer on: **10/10/2008 at 8:00:00 PM**.*

File Name	File Creation Timestamp	EXIF Timestamp
IMG_300	**10/10/2008 8:00:00 PM (changed again)**	01/01/2008 11:11:10 PM (unchanged)

b. Summary of the Finding

The range of photos on the hard drive, including the alleged contraband, have EXIF timestamps and other metadata that suggest they originated from the camera and memory card in 2005. For specific groups of photos, such as the twenty individual photos in the range IMG_0081 through IMG_0100[17] (Photo Files 81–100), there are corresponding file names on the memory card with matching timestamps from 2005, such as the **file creation timestamps** on the memory card matching the **EXIF timestamps** on the hard drive, indicating that these files were originally saved to the memory card in 2005 and later transferred to the hard drive.

[17] This camera automatically names files sequentially in the format "IMG_," followed by a number, where the number increases with each photo taken, e.g. IMG_0001, IMG_0002, ec.

These twenty photo files on the memory card, IMG_0081-0100, had been deleted but were partially recovered using forensic software. While no visual images for these files could be recovered, the file names and file system timestamps recovered suggested these were the original files that were later backed up to the hard drive. This apparent alignment between the hard drive and memory card supported the government's argument that the photos on the hard drive, including the alleged contraband, were all taken by the seized camera in 2005.

However, our analysis in Technical Finding #8 reveal **that the twenty individual files in the range IMG_0081 through IMG_0100 on the memory card were planted there using a computer**, and their file system timestamps were manipulated, making them falsely appear as if the camera placed them there in 2005. We determined that the only plausible explanation is that these files were retrofitted onto the memory card with manipulated timestamps to create the illusion that the camera saved them in real-time in 2005, supporting the government's narrative. As previously discussed, it is even possible these are not photo files but merely files renamed to look like photo files from the Canon camera.[18]

c. How We Determined the Files Were Planted

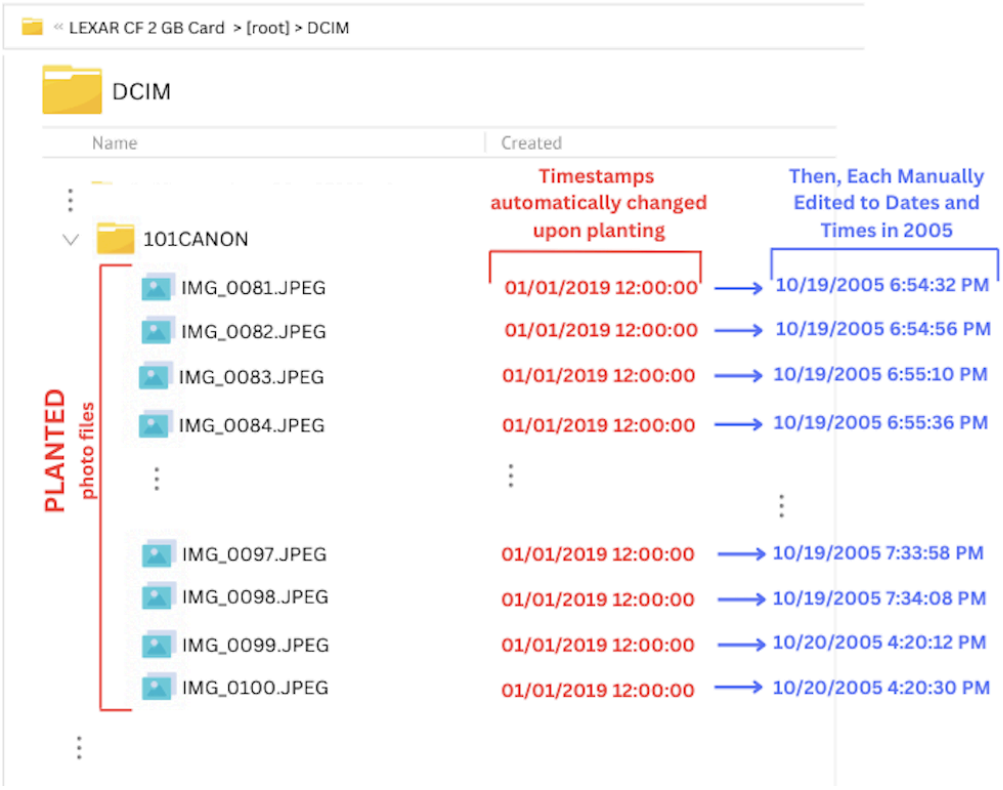
Testing by Stephen Bunting, one of the undersigned experts, on a Canon EOS 20D (with the same firmware, 2.0.2., as in this case) confirmed that these files could not have been written to the memory card by the camera itself. This camera has a specific way of saving files to certain locations based on available space, and the placement of IMG_0081-0100 and IMG_0224-0243 does not align with how the camera is capable of operating.[19] In other words, contrary to how it appears, **the camera did not place them on the memory card. They were added to the memory card using a computer.**

Further, based upon this conclusion, we determined that after planting the photos, someone "subsequently edited their creation dates" (Joint Report at ¶15(a)) because the file system creation timestamps for IMG_0081-0100 match their hard drive namesakes and the file system creation dates for IMG_0224-0243 match their EXIF creation timestamps on the camera card. Otherwise, these timestamps would have reflected the date and time of the planting event.

This process of timestamp manipulation is visually represented in the diagram below, for a **hypothetical** transfer date and time of 1/1/2019 at 12:00:00 PM, where the computer would automatically update the file creation timestamps to that date and time after the planting.

[18] *See* Dr. Kiper's Report, Doc. 1169-1 at PageID # 21355
[19] *See* Mr. Bunting's Report in Appendix B of the Joint Report.

Diagram 4: Visual Representation of the Planting and Timestamp Manipulation



Based on the same analysis, in Technical Finding #9, we determined that 17 files (IMG_0224-0243), dated beginning roughly three months after the photos on the hard drive but appearing to be part of the same overall series, were also planted on the memory card, and their timestamps were subsequently manipulated, making it falsely appear as though the camera saved them in real-time. This continuity further reinforced the government's alleged 2005 timeline.

d. Why This Matters

Using a computer to insert and precisely modify these photo files on the memory card is as unnatural as taking a car back to the assembly line for an oil change —something that, in our experience, no normal user would ever do.

We determined that the only plausible explanation for these manipulations is to retrofit the memory card with planted files to support the narrative that the seized camera took the photos found on the hard drive in 2005.

e. Status

Technical Findings #8 and #9 were included in the defense's Motion for Reconsideration (Doc. 1225), which the government opposed (Doc. 1229), but did not include a rebuttal from Loveall or any other expert. Therefore they are uncontested.

4. The Last Accessed Dates of 29 Photo Files on the Memory Card Were Intentionally Altered by a Computer (Uncontested)

a. Background

Photos 21-42 are the earliest photos on the memory card and are significant because their numbering sequence precedes the first set of photos on the hard drive (43-58). This makes it look like the photos across devices are part of one continuous sequence: the camera saved them to the memory card, and later, some of them were transferred to the hard drive. In Technical Finding #10, we found that the "last accessed dates" of Photos 21-42 were tampered with.

A last accessed date records the most recent time a file was opened or interacted with. Stephen Bunting determined, through testing the same camera and firmware as in this case, that this particular camera does not update last accessed dates when photos are viewed on the camera itself; similarly, when the camera is connected to a computer via USB, the last accessed dates remain unchanged. These timestamps only change if the memory card is accessed directly through a computer's card reader or slot.

b. The Anomaly

In Technical Finding #10, we observed that most photos in the range 21-42 have a last accessed date of October 16, 2005, two days after their creation, but two photos—29 and 42—show an earlier last accessed date of October 14, 2005.

Since all the photos were stored in the same folder and were active (non-deleted) at the same time, any computer access should have updated the last accessed dates for all of them, not just all but two of them. This inconsistency cannot be explained by normal camera use or simply connecting the camera to the computer, leading to the conclusion that someone directly accessed the memory card and manually altered the last accessed dates using a computer. This pattern of anomaly was also observed in Technical Finding #11, affecting photo files 193-199, in which we also concluded manual tampering of last accessed dates.

c. Why This Matters

In our experience, altering last accessed dates is highly unusual and not something a typical user would do, let alone on a camera memory card. Users might delete photos or transfer them, but not manipulate access dates. The selective modification of these timestamps constitutes intentional tampering. Notably, the last accessed dates on the memory card are in 2005 and roughly match the alleged photo capture time frame.

d. Status

These findings were also included in the defense's Motion for Reconsideration, which the government opposed, but did not include a rebuttal from Loveall or any other expert. Therefore they are uncontested.

5. Manipulation of Timestamps in Folder Names (Uncontested)

In Technical Finding #6, we determined that the names of folders on the hard drive, which correspond to specific dates and times and appeared to indicate when photos were downloaded in 2005, were manually manipulated. Loveall did not contest this finding. He simply stated, "it is of course possible to rename files and folders and any computer user may do so," failing to address the deliberate manipulation of folder names, which falsely suggested the photos were downloaded at the specific dates and times in 2005 indicated in the folder names. (Loveall Report at ¶ 16)

6. Manipulation of Last Modified Timestamps, Apparently to Simulate an Automatic Daylight Savings Time Adjustment in 2005 (Contested)

a. Our Finding (Technical Finding #4)

We determined that a two-hour shift between the file system last modified timestamps and EXIF created timestamps was present in only 11 photos in a single folder and in no other photos on the hard drive. We determined that this is best explained by someone inadvertently overlooking this folder while doing the manipulation. Further, we found that this change "most plausibly happened because they were attempting to mimic an automatic Daylight Savings Time adjustment from 2005 but made errors in the process."[20]. In our experience, a normal user would not make these changes, which falsely supported the alleged 2005 timeframe.

b. Evaluation of Loveall's Rebuttal

Loveall's rebuttal is hypothetical, unsupported by evidence, and does not explain the observed two-hour discrepancy.

Summary of Loveall's Response	**Critique of Loveall's Response**	**What a Proper Response Should Look Like**
Loveall claims the timestamp changes are likely due to: - Manual or automatic changes to device clocks in 2005. - A 2006 Windows update introducing dynamic Daylight	**No Evidence**: Loveall does not test or demonstrate any of his claims. **The 2006 Update Does Not Apply**: This update does not retroactively affect existing	A valid response would: 1. Simulate a pre-2006 Windows environment with files matching the original (unshifted) timestamps.

[20] *See* Joint Report ¶ 9.

Savings Time (DST) time zones. (Loveall Report at ¶¶ 11-14).	files. It only applies to files created afterward. **Fails to Specifically Explain the Anomaly**: Loveall does not explain how such an update would account for the observed two-hour shift followed by exact alignment of last modified and EXIF timestamps.	2. Apply the 2006 Windows update and document whether it reproduces the two-hour shift and timestamp alignment. 3. Provide detailed steps, including screenshots and system settings, to ensure transparency and reproducibility.

Loveall's response lacks scientific validity and fails to explain the timestamp anomalies. It is simply speculative. As such, our finding that these last modified timestamps were manually manipulated stands.

7. Manual Manipulation of Timestamp/Metadata of Photo 175 (Contested)

a. Our Finding (Technical Finding #5)

In Technical Finding #5, we determined that the metadata of Photo 175, located on both the camera card and on the hard drive, had been manually manipulated. In this instance, the manipulated metadata refers to the EXIF data, which is part of the photographic *content*. The identical *last modified* timestamps indicated the photo had not been modified during its copy from the camera card to the computer and then to the external hard drive However, the EXIF data on the hard drive copy of Photo 175 indicated that it was modified by Photoshop Adobe Elements. Any change in a photograph's EXIF data will necessarily change its last modified timestamp, absent human intervention. Based on these facts, we determined that the *last modified* timestamps of the Photo 175 copies were artificially synchronized to be the same, even though the EXIF data on the hard drive copy indicates the file had been modified. This synchronization of timestamps suggests intentional tampering to conceal file manipulation.

b. Evaluation of Loveall's Rebuttal

Loveall's rebuttal is unsupported. He claims Adobe Photoshop Elements could have altered metadata without updating the modification date but provides no evidence to substantiate this claim.

Summary of Loveall's Response	**Critique of Loveall's Response**	**What a Proper Response Should Look Like**
Loveall claims that in Adobe Photoshop Elements, selecting "Change to a	**No Evidence**: Loveall does not test or demonstrate this behavior or provide	A valid response would: 1. Conduct controlled tests

specified date and time" and clicking 'OK' without entering a new date can alter some internal metadata without updating the *last modified* timestamp. (Loveall Report at ¶ 15).	screenshots to support his claim. **Inconsistency**: Loveall's explanation relies on intentional use of timestamp manipulation features, undermining his claim that no manual alteration occurred.	with Adobe Photoshop Elements to see if metadata can be altered without updating the *last modified* timestamp. 2. Document each step taken, such as using the "Change to a specified date and time" feature and clicking 'OK.' 3. Verify whether the observed timestamps match the results of these tests. 4. Provide reproducible evidence, like screenshots or logs, to support the findings.

Loveall's rebuttal lacks scientific rigor, provides no proof, and inadvertently reinforces the finding of manual manipulation by suggesting intentional use of timestamp-altering software. Thus, our finding stands.

8. Manual Manipulation of Photo Files 93-97 on the Memory Card (Contested)

a. Our Finding

Technical Finding #1 identified that the photo files IMG_0093-97 on the memory card contained the thumbnails of photo files 180-183, which depicted a different subject. We determined that this anomaly indicated intentional manipulation of the files and their metadata.

Additionally, Technical Finding #8 conclusively shows that IMG_0093-97, as part of the range IMG_0081-100, were planted on the memory card using a computer, with timestamps intentionally altered to create the appearance of real-time camera use in 2005. **Thus, this finding is subsumed by and more fully explained by the deliberate planting and manipulation described in Technical Finding #8**.

b. Evaluation of Loveall's Rebuttal

Loveall's response relies on hypothetical scenarios, lacks supporting evidence, and does not align with the observed data or behavior of the memory card and camera.

Summary of Loveall's Response	**Critique of Loveall's Response**	**What a Proper Response Should Look Like**

Loveall argues that the anomalies in IMG_0093-97—where thumbnails depict a different subject than the actual photos—can be explained by normal FAT file system behavior. Specifically, he claims: - Older deleted files may be overwritten by newer ones, causing metadata misattribution, which would explain the mismatched thumbnails. (Loveall Report at ¶¶ 5-8). - This behavior is "particularly true" when a memory card is full. ((Loveall Report at ¶ 5).	**Unsupported Hypothesis:** Loveall provides no testing, demonstrations, or evidence to support his claims. He does not cite the actual data on reports or the memory card, despite having access to the memory card and the two forensic copies. **Misleading Capacity Argument:** Loveall claims the issue is "particularly true" when the memory card is full, but testing shows the card never exceeded 6% of its capacity. The farthest-used photo location is only 120 MB into a 2 GB card.[21] His explanation is irrelevant to this case. **Wrong File System Explanation:** Loveall's explanation applies to NTFS file systems, not FAT-16, which is used by this card. FAT-16 zeroes out all pointers except the first segment of a file upon deletion[22], making fragmented or partially recovered files impossible. Only contiguous files can be accurately recovered on FAT-16. **Inaccurate Camera Behavior:** Loveall's description and diagrams of file overwriting do not match the Canon EOS 20D's cluster	A proper response would: **1. Examine the Files**: Use forensic tools to inspect where the data from IMG_0093-97 and IMG_0180-183 are stored on the memory card. Check if parts of IMG_0180-183 are overlapping with or pointing to the same space on the memory card as IMG_0093-97. **2. Simulate the Camera's Overwriting Behavior** : Use the same camera model (Canon EOS 20D) with matching settings and memory card type and try to reproduce a situation where thumbnails from a newer photo, like IMG_0180, accidentally end up in the file space of an older photo, like IMG_0093, as Loveall suggested. **3. Recover Deleted Data**: Use forensic tools to recover deleted files and see if the recovered thumbnails are incorrectly matched with older files. **4. Document Everything**: Provide clear records of all steps taken, including screenshots and logs, so that the process can be repeated by others to verify the

[21] *See* Joint Report ¶ 14 and Booth's FTK Report, Government Exhibit 521A - Replacement.
[22] "The Starting Cluster is an unsigned integer representing the Logical Cluster Number in which the file starts. It is stored in two separate areas of the Directory Entry, as FAT was originally designed for small volume sizes." See *FAT File System Section*, 2021 IACIS Basic Computer Forensic Examiner Manual, at Bates No. 145; See also *Id* at Pg. 159.

	writing behavior, as detailed in Stephen Bunting's previously submitted report.[23]	findings.

V. Conclusion

The above findings constitute a clear and extensive pattern of data falsification on both the camera's memory card and hard drive, with the apparent intent of creating the impression that the photos on the hard drive, including the alleged contraband, **were taken in 2005** and **using that particular camera**, which was precisely the government's narrative.

Additionally, as shown above, Loveall's rebuttals to the select findings he addressed fail to scientifically refute any of them. His responses were speculative, unsupported by evidence, and in some cases demonstrably false.

Further, we previously found, and reaffirm our conclusion that:

> "Given admitted government misconduct, including violating evidence protocols, providing evidence to unidentified and unauthorized personnel, and altering the original camera card, the involvement of government personnel in this evidentiary fraud is inescapable – an unprecedented finding in our combined 150+ years of forensic experience." (Joint Report ¶ 16).

Signature: Signed by: 0B3F4F5049A24DD...
Executed on: 11/28/2024
Name: **Dr. James Richard Kiper, Ph.D.**
Background: Former FBI Special Agent, Computer Forensic Examiner, and Unit Chief at the FBI Academy, 20 years' service to the FBI

Signature: Signed by: 75268C7A16C04A2...
Executed on: 11/28/2024
Name: **Stacy Eldridge**
Background: Former FBI Senior Forensic Examiner, 10 years' service to the FBI

[23] *See* Joint Report, Appendix B

Signature: DocuSigned by: Mark Bowling 0F0676862144440...
Executed on: 11/28/2024

Name: **Mark Daniel Bowling**

Background: Retired FBI and OIG Special Agent and Forensic Examiner and Former FBI Assistant Special Agent in Charge, FBI Inspector in Place, and Cyber Program Manager, 20 years' service to the FBI

Signature: DocuSigned by: William Odom A2537825AE824DC...
Executed on: 11/28/2024

Name: **William Odom**

Background: Former FBI Special Agent and Forensic Examiner, Manager of the FBI Forensics Lab in Houston; 5 years' service to the FBI

Signature: Signed by: B116E4E862A04F0...
Executed on: 11/28/2024

Name: **Steve Abrams, J.D., M.S.**

Background: 25+ years in digital forensics, worked 1,500+ cases, served 11 years as a South Carolina State Constable, for the US Secret Service.

Signature: DocuSigned by: ADA3D90C6B7D4FF...
Executed on: 11/28/2024

Name: **Stephen Bunting**

Background: Former Captain of the University of Delaware Police, created the University of Delaware Police's digital forensics unit; trained hundreds of examiners and authored five textbooks in the field of digital forensics.

Signature: Signed by: Wayne Norris BD1865C1FB84496...
Executed on: 11/27/2024

Name: **Wayne Norris**

Background: 60+ years of software development experience across 35 operating systems, the government's lead software development expert witness in the landmark *Microsoft vs. Commissioner of Internal Revenue* case, 36+ years of computer forensic expert experience.