



## KiperteK, LLC

"Making Sense of It All"

2800 South Adams Street #6971, Tallahassee, FL 32314

Phone: 954-995-3811 / E-mail: [info@kipertekusa.com](mailto:info@kipertekusa.com)

---

### EXPERT REPORT

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

FBI Special Agent (Retired) and Forensic Examiner

April 8, 2025

#### **Professional Background**

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics. In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners in the FBI's Computer Analysis Response Team (CART) program. 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. Currently I provide consulting services and training in the areas of cybersecurity and digital forensics.

#### **Review of the Facts**

After being retained in the case *U.S. v. Cherwitz, et al.*, No. 23-CR-146 (DG), I reviewed relevant information pertaining to the government's collection and possession of a Western Digital My Passport external hard drive, serial number WX31A41F2566 (hereinafter, the "WD HD"). Specifically, I have reviewed the physical and electronic chains of custody for the hard drive, an e-mail conversation identified as GX 3500-ABL-3, an affidavit supporting a search warrant for the hard drive, and various legal communications.

#### **Key Findings**

1. The FBI agent who collected the WD HD circumvented the FBI's CART procedures and violated FBI's Digital Evidence Policy Guide (DEPG).
2. The FBI did not follow CART standard operating procedures (SOPs) while examining the WD HD.
3. The WD HD, currently in the possession of the government, likely holds evidence of the government's access of the hard drive and the modification of its contents.
4. The WD HD, currently in the possession of the government, likely holds evidence relevant to the defendants in this case.

**Finding 1: The FBI agent who collected the WD HD circumvented the FBI's CART procedures and violated FBI's Digital Evidence Policy Guide (DEPG).**

Large FBI offices like the New York Division have a centralized evidence control and storage facility sometimes referred to as the Evidence Control Room (ECR). Normally, evidence is collected by a special agent at a search site, or from a cooperating witness, and a description of the collected items is entered into Sentinel, the FBI's case management system. Once the evidence is collected FBI policy allows the agent up to ten calendar days<sup>1</sup> to officially document the collection, followed by physically turning over the evidence to the ECF, along with its chain of custody.

In the case of digital evidence, the case agent submits a written request (a "CART request") to have the evidence examined by a CART examiner. The assigned CART examiner would check out the relevant evidence item from the ECR, sign the chain of custody, and then proceed to examine the evidence in accordance with CART procedures. The most critical forensic procedure is that of connecting the evidence to a write-blocking device, through which the evidence can be viewed and a forensic copy (or forensic image) can be created to preserve the evidence.

As a former CART examiner, trainer, curriculum developer, and instructor developer in the FBI CART program, I can attest that all CART examiners are trained in the above procedures, which are part of the CART Standard Operating Procedures (CART SOPs). Having served as the Chief of the Investigative Training Unit at the FBI Academy, I can also attest that FBI Special Agents are trained to follow their part the above evidence handling process, which is designed to prevent unauthorized (and possibly destructive) access to digital evidence.<sup>2</sup>

Unfortunately, Special Agent Elliot McGinnis did not follow these procedures. According to the chain of custody, SA McGinnis received the WD HD on 04/15/2024 and retained sole custody of it for more than ten weeks until he finally checked it into the ECR on 06/26/2024. During those weeks, SA McGinnis accessed the WD HD at least once, and likely several times because, in his own words, he "[REDACTED]." <sup>3</sup>

In his communications I did not observe SA McGinnis identify himself as a Special Agent Forensic Examiner (SA/FE), nor did I see that he was authorized to review original digital evidence as a "CART Tech," who is trained in digital evidence preservation. Therefore, it is

---

<sup>1</sup> 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>)

<sup>2</sup> *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."

<sup>3</sup> See e-mail message from SA McGinnis to Randy Lopez, sent 05/03/2024. In a subsequent e-mail message on 05/21/2024, SA McGinnis stated, "[REDACTED]" This statement implies that he was continuing to access the WD HD and was now confident the files could be extracted.

highly likely that SA McGinnis accessed the WD HD *without a write-blocking device*, and in doing so necessarily altered the evidence.<sup>4</sup>

Rather than allowing CART to first preserve the evidence against alteration, SA McGinnis circumvented the FBI's digital evidence procedures by maintaining custody of the WD HD for several weeks while he accessed and irreversibly altered the contents of the original evidence.

**Finding 2: The FBI did not follow CART standard operating procedures (SOPs) while examining the WD HD.**

As stated previously, all digital evidence obtained by the FBI is first sent to CART for preservation prior to anyone else reviewing the evidence. CART examiners preserve the evidence by connecting it to a write-blocking device<sup>5</sup> and creating a forensic image<sup>6</sup>, which is a bit-by-bit digital replication of the contents of the evidence media. After completing the imaging process, the CART examiner then verifies<sup>7</sup> the forensic image, ensuring that all data was copied correctly. After that, the examiner stores<sup>8</sup> the *original* physical evidence and then applies forensic software tools to the evidence *copy* (the image) in order to view and extract data relevant to the investigation. After the forensic image is created, therefore, there is no need to handle the original evidence media again until it is presented at trial.

Unfortunately, FBI employees apparently failed to complete these critical procedures while examining the WD HD. Although the FBI's Sentinel record shows that the WD HD was received by CART on 08/27/2024, the chain of custody indicates it was not checked out from the ECR and given to a CART examiner until 09/03/2024. If the CART examiner had followed CART SOPs and created a forensic image of the evidence at that time, then there would be no reason to ever handle the original WD HD again. However, the WD HD was indeed checked out of the ECR several more times during the ensuing months, with no compelling reason to do so.

Special Agent Daniel Schmidt, the search warrant author and affiant, checked out the WD HD from the ECR on 09/03/2024 at 12:22 PM and then immediately turned it over to CART Forensic Examiner Vincent Radice at 12:26 PM. FE Radice kept the device until the following day, when he returned it to the ECR at 3:25PM. If he had followed CART SOPs, then FE Radice would have created and verified a forensic image of the WD HD and returned the original device to the ECR. All subsequent review and examination would have been conducted on the *forensic image*, rather than on the original WD HD. However, this is not what happened.

The day after FE Radice returned the WD HD to the ECR, SA Schmidt checked it out of ECR on 09/05/2024 and kept it for more than a week before returning it to the ECR on 09/13/2024. What

---

<sup>4</sup> Without the use of an intervening write-blocking device, the simple act of attaching the WD HD to a computer will result in, at a minimum, file accessed dates being changed. Many more alterations occur as the user opens and views files on the device.

<sup>5</sup> CART SOP section 4.3 Write Protection Procedure.

<sup>6</sup> CART SOP section 4.5 Imaging Procedure.

<sup>7</sup> CART SOP section 4.7 Verification of Imaged/Copied Data Procedure.

<sup>8</sup> 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."

he did with the device is anyone's guess. In the chain of custody SA Schmidt gave no operational reason for why he needed to handle the original evidence again. SA Schmidt checked out the WD HD again on 10/23/2024 at 9:45AM and immediately turned it over to CART FE Radice at 9:51AM. FE Radice again kept it for a day before returning it to the ECR, providing another opportunity to image the WD HD and remove the need to handle the original evidence again.

However, it is apparent that FE Radice did not image the WD HD because SA Schmidt checked it out again on 10/29/2024 (the date he was granted the search warrant) and kept it for two weeks before returning it to the ECR on 11/14/2024. Again, he provided no justification in the chain of custody for doing so. On 12/04/2024 CART FE Radice checked out the WD HD himself and kept it until 12/10/2024, which provided a *third* opportunity to image the original device and protect it from unauthorized handling.<sup>9</sup> However, SA Schmidt checked it out again on 02/11/2025, again without justification, and kept it for three days before returning it on 02/14/2025.

In the introduction of his search warrant affidavit, SA Schmidt makes no mention of any CART certifications or technical training that would have authorized him to review original digital evidence as he done several times in this case. In paragraph 26 he makes a vague reference to the "[REDACTED]" of CART in reviewing "[REDACTED]," but he does not describe what he did to the device during the times he checked it out *without CART assistance*.

For example, in paragraph 27 of the search warrant affidavit SA Schmidt states that he had discovered a backup volume on the WD HD on 10/10/2024:

[REDACTED]

The date of this discovery is questionable, because according to the chain of custody the WD HD was in stored in the ECR from 09/13/2024 to 10/23/2024. Neither SA Schmidt nor FE Radice had access to the original device during that time.

It is possible that FE Radice had created a forensic image of the WD HD and that SA Schmidt was reviewing that copy of its contents on 10/10/2024. But if that were the case, then why did SA Schmidt check out the original WD HD again from the ECR on 10/23/2024 and immediately turned it over to FE Radice, who kept it for a day before returning it to the ECR? And why did SA Schmidt check it out again on 10/29/2024 (the date of the search warrant) and keep it for more than two weeks? And why did he check it out again on 02/11/2024 and keep it for three days? *Again, the existence of a verified forensic image would have precluded the need to ever review the original evidence again.*

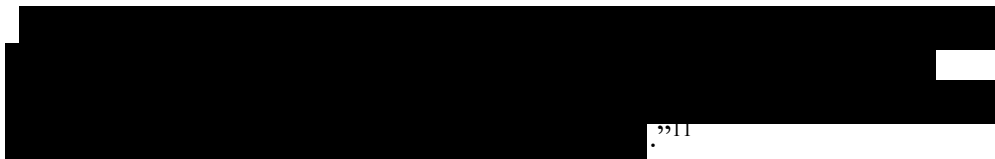
---

<sup>9</sup> *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.'"

<sup>10</sup> Search Warrant Affidavit for the WD HD, page 7, paragraph 27.

In my 20 years of FBI service as a Special Agent, I have never seen such chaotic activity in a chain of custody for an evidence item. There is simply no justification for SA McGinnis, who collected the WD HD, and SA Schmidt, who authored the search warrant for its contents, to have multiple weeks of unsupervised access to the original digital media. Neither of these employees were authorized or qualified to review the contents on the original device, and it is unclear whether FE Radice ever followed CART SOPs to preserve it from alteration.

Neither the FBI investigating agents nor the CART forensic examiner followed established protocols with respect to the examination of the WD HD. With so many unauthorized reviews of the original digital evidence – by untrained and unauthorized FBI agents – it is highly likely the WD HD was altered while in the custody of the FBI. This finding challenges the claim of SA Schmidt in his sworn search warrant affidavit:



**Finding 3: The WD HD, currently in the possession of the government, likely holds evidence of the government's access of the hard drive and the modification of its contents.**

Based on the previously cited documented examples of unauthorized access by FBI agents, there is a strong possibility that the contents of the WD HD were altered while in the custody of the FBI. If I were to have access to the WD HD, or to a verified forensic image of the WD HD, I would be able to extract several types of information relevant for determining whether the FBI accessed and altered the contents of the external hard drive. Relevant data would include the following:

- **Active files** – These are files that are being actively used by the computer and are available to the user. Active files could include documents, spreadsheets, multimedia, executable applications, and application support files. The WD HD contains a file system that manages the physical location of files and their metadata – including timestamps, authors, and related devices – that record how the files were used, by whom, and when. Any file that has a created date, modified date, or accessed date after the date the WD HD was received by the FBI (04/15/2024) would demonstrate to a scientific certainty that the FBI has accessed the WD HD without a write-blocker and modified its contents.
- **File versions** – Some applications retain stored copies of files, either as a result of application crashes or by manual intervention, as in tracking changes. Stored versions of files can provide the same types of information as the final versions of such files, and may yield clues of tampering.
- **Deleted files** – When a file is deleted, its data contents and metadata are not immediately destroyed. Deleting a file simply gives the file system the permission to overwrite the

---

<sup>11</sup> Search Warrant Affidavit for the WD HD, page 8, paragraph 30.

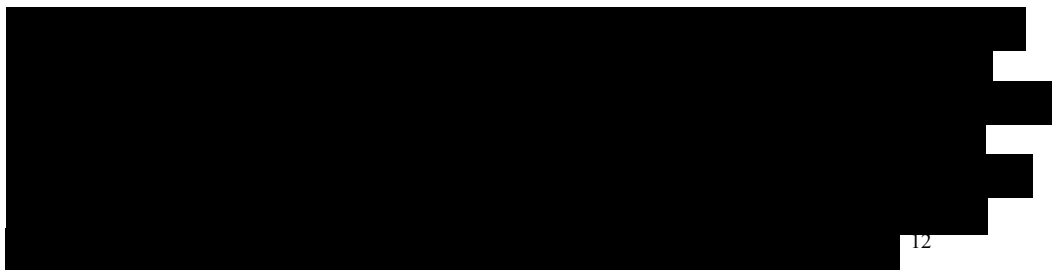
data in the future, subject to certain rules and conditions. Many deleted files are fully recoverable, and may contain the same types of data (and metadata) as active files.

- **Embedded Metadata** – Some files may contain special information, such as contributing authors or a specific printer that was used. Digital photographs often contain information (EXIF data) about the camera, camera settings, GPS location information, and what application was used to edit the photograph.
- **Log files** – While some logs are generated by the computer system, many applications generate their own log entries that record actions and events, along with the dates they occurred. Logs can be found in active files, hidden files, and deleted files.
- **Unallocated space** – This represents areas of the hard drive that may have lost its data mapping due to being overwritten or partially overwritten by new files. However, remnants of past files can still be recovered from this area and related to other information.

Any of this information, and much more, may be retrieved through a forensic analysis of the WD HD or of a forensic image of that device. Again, any discovered information that corresponds to FBI-related people, equipment, processes, or any timestamp occurring after the date the FBI accepted custody of the WD HD, would necessarily implicate the government’s access and alteration of original evidence.

**Finding 4: The WD HD, currently in the possession of the government, likely holds evidence relevant to the defendants in this case.**

From my review of the facts, it seems that many of the allegations against the defendants pertain to actions and events that may have occurred during a specific period of time when the defendants had roles at the OneTaste organization. This timeline necessarily intersects with information provided by one of their accusers, namely “Jane Doe #1,” the owner of WD HD described in the search warrant affidavit. In fact, the affidavit describes how this information was discovered on the WD HD:



The above paragraph describes information that is relevant to the defense because:

- Both “Jane Doe #1” (the original WD HD owner) and her “Sister” (a recent custodian of the WD HD) gave the FBI consent to search contents for information related to Jane Doe

---

<sup>12</sup> Search Warrant Affidavit for the WD HD, page 7, paragraph 27.

#1's time at OneTaste, *which necessarily corresponds to the time that the defendants served in their roles at OneTaste*;

- The FBI confirmed they identified those materials, which are within the scope of the granted consent, located in the contents of the WD HD; and
- The materials included "[REDACTED]" *and therefore to the defendants' time at OneTaste*.

From my review of the facts, I understand that the observed "[REDACTED]" relate not only to Jane Doe #1's time at OneTaste, but also to the time period when the defendants were involved at OneTaste. A forensic review of these WD HD documents, including any tracked changes and versioning, is required to establish their authenticity.

The next paragraph in the affidavit describes SA Schmidt's discovery of what appeared to be a system backup of an entire computer:

[REDACTED]

I will set aside the implausibility of SA Schmidt having made this discovery on the "SUBJECT DRIVE" on a date when it was in fact locked up in the ECR, because I have already addressed this anomaly. However, what I find bizarre is SA Schmidt's characterization that the materials in the discovered "back up" had *exceeded the scope of the consent*, when he had just described the information he observed in the backup, that is, "[REDACTED]" This description is clearly a perfect match for the description of files that *would be in the scope* of the granted consent, which was "[REDACTED]"<sup>14</sup> I cannot speculate as to why SA Schmidt requested search warrant authority for precisely the type of information he had already obtained by way of consent.

Regardless of the specific legal authority, the fact remains that the WD HD was found to contain "an entire back up of Jane Doe #1's computer," which included "files from the time period during which Jane Doe #1 was involved at OneTaste." This specific time period, as I have already pointed out, is necessarily the time period corresponding to the defendants' time at OneTaste, and is therefore relevant to their defense.

Moreover, a full computer backup would contain many more types of information than that of a simple file storage container (as I described in Finding 3). A system backup could include additional artifacts of user activity, including:

---

<sup>13</sup> Search Warrant Affidavit for the WD HD, page 7-8, paragraph 27.

<sup>14</sup> Search Warrant Affidavit for the WD HD, page 7, paragraph 26.

- Internet browsing history, “cached” files, and downloaded files.
- Conversations generated by and saved in e-mail and messaging accounts.
- Event logs, including login accounts and times.
- Prefetch files, which record the uses of specific applications.
- Saved memory artifacts (e.g., pagefile.sys, hiberfil.sys) that could contain remnants of user activity, including viewing and authoring of documents.
- Windows registry, which is a vast database repository of “user attributable” information, including most recently used applications, documents, folders, attached devices, web sites visited, keyword searches, and much more.

Because the time period and content of the WD HD files observed by SA Schmidt correspond to that which are relevant to the defendants, it would be appropriate for the government to provide a verified forensic image of the device to the defense team. Moreover, a rigorous forensic analysis of the WD HD resulting in the recovery of data described in this paper is likely to yield exculpatory information owed to the defendants.

### **Additionally Requested Information**

In addition to a verified forensic image of the WD HD, there are a number of documents that should also be provided to the defense team:

- **Consent to Search form** – According to the search warrant, the consent to search was provided by “Jane Doe #1 and the Sister,” and the scope of the consent was “information related to Jane Doe #1’s time at OneTaste.”
- **CART Request** – Written by the case agent and saved into the CART Database, this document sets forth the legal authority and the specific work requested from CART.
- **CART Examination Notes** - In this document, the CART examiner records every step taken during the collection, preservation, examination, analysis, results, and reporting of the digital evidence item. In the Examination Notes, CART FE Radice would have recorded each time he received the WD HD, exactly what he did with it, and which tools he used.

### **Conclusion**

An important rule of handling the FBI’s digital evidence is the requirement that only fully qualified and trained forensic examiners in CART are allowed to access original digital media. In this case, however, unauthorized FBI agents repeatedly accessed the physical WD HD, rather than the forensic copy (or image) that was supposed to have been generated by a certified CART examiner. The repeated violations of FBI CART protocols and of the FBI’s Digital Evidence Policy Guide likely resulted in spoliated evidence that cannot be relied upon for court purposes. However, it is my opinion that the verified forensic image of the WD HD should still be provided to the defense team, as the results of its analysis could include exculpatory evidence, as well as data that informs the court’s assessment of the government’s overall conduct and the integrity of the evidence they present.



These findings represent my knowledge and analysis of the information that has been provided to me to date. I reserve the right to change my opinions based on new information I may receive in the future.

Respectfully Submitted,

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