MANAGEMENT REVIEW

I was asked by Defendant's counsel to estimate the scope of work required to produce the data alterations initially discovered in the Government's evidence by Dr. Kiper.

I divided this analysis into two parts, described as "PROJECTS" so as to use the terminology of the Project Management community.

- In the first Project, I analyzed a possible scenario for the creation of altered data on the CF Card [1B15a].
- In the second Project, I analyzed a possible scenario for the creation of altered data on the WD HDD [1B16].

It should be noted that these two Projects actually occurred in the reverse time order of my presentation here. Dr. Kiper used this time order in order to make the most logical sense of the actual forensic results. I analyzed them in this same order so as to match the order used by Dr. Kiper in his analysis.

As with any such report, this one is based on assumptions driven by:

- Examination of artifacts;
- Analysis of schedules;
- Analysis of testimony; and
- Considerations of technologies.

The assumptions upon which this analysis and estimate are based are classified by artifact, as listed below.

MY ANALYSIS SHOWS A TOTAL ESTIMATED POTENTIAL EFFORT OF 128 HOURS BY INDIVIDUALS WITH FOUR DIFFERENT SPECIALTIES.

PROJECT 1. Lexar CF ["Compact Flash"] Card 1B15a also cataloged as GX 524 [alternatively referred to in Dr. Kiper's reports as an "SD" or "Secure Digital" Card]

This is an evidence item, cataloged as 1B15a or GX 524, consisting of an SD card that had been removed from a Canon camera, with abbreviated name SD Card. Below is a brief timeline of events pertinent to this analysis:

On 3/27/18, the CF card was seized, along with the camera and other devices, including the WD HDD.

From 7/10/18 to 7/27/18, Case Agent Rees had custody of the device, outside of Evidence Control. From 9/19/18 to 9/26/18, Case Agent Lever had custody of the device, during which time the CF card was altered (see Technical Finding #3 in Dr. Kiper's Technical Report). Thus, during 24 calendar days when the CF card was checked out of Evidence Control, and in the custody of Case Agents, it was modified. This was several months before the SD card was checked into CART, on 2/22/19, and imaged and analyzed by FE Flatley. (see Dr. Kiper's Process Findings.)

From 2/22/19 to 6/7/19, Flatley held the CF card. For the subsequent three days up until Booth received and then re-cloned the SD card, which arrived to him in an unsealed cellophane bag (see Dr. Kiper's Process Findings), three FBI personnel had custody of the CF card: SA McGinnis, SA Mills, and FE Booth. Based on the technical findings, it is likely that additional alterations took place by this time.

Question Posed to Me: I was asked to examine the hypothetical work needed to convincingly yield the artifacts described above. I identified only a single subtask.

Assumptions:

I made working assumptions that anyone doing this work was trained on standard computer subjects and on evidence handling, and that they had an expectation of "medium level" scrutiny for the evidence, a level below that of a highly skilled forensic investigator.

I also made a working assumption that anyone doing this work would attempt to minimize the amount of data alteration performed, since each alteration added risk of detection during an intensive search.

Based on the evidence, I further assumed that the Government had deleted the errors made in the fabrication of the WD HDD, which occurred chronologically earlier, and thereby a decision was made to manipulate data on the CF card so as to make the data on the WD HDD appear more credible. Given that the purpose was to essentially "clean up" what could be cleaned up on the HDD, and that the schedule available for it was very limited, this work was likely undertaken under time pressure. I attribute the errors made during the alteration that allowed Dr. Kiper to discover the alteration to time pressure and lack of access to the HD.

Discussion

This process subsumes KEY FINDINGS 1, 2, and 3 by Dr. Kiper. His findings 4, 5, 6, and 7 are the subject of the second analysis in this report, below.

PROJECT 1 ESTIMATED TOTAL HOURS:

32 HOURS by a SENIOR FORENSIC INVESTIGATOR

PROJECT 2. WD HDD 1B16 also cataloged as GX503 [ORIGINAL]

At the outset there existed an evidence item, cataloged as 1B16 and also as GX 503, consisting of a Western Digital hard drive, with abbreviated name WD HDD.

Question Posed to Me: I was asked to examine the hypothetical work needed to convincingly add CP files to a version of WDD HDD 1B16 / GX 503 during the 134 days between the date it was taken into custody until it was transferred to FET VD.

Assumptions:

I made the same working assumptions for this Project as for the one above, including time pressure as a significant constraint.

As a consequence of these working assumptions, I analyzed a scenario in which:

A. The drive was first analyzed, as a precaution, to determine the presence of deleted files, hidden files, file fragments, or other items whose content should be known prior to alteration of evidence. This could be done with either FTK, the tool used by the FBI itself, the freeware tool AUTOPSY, or other forensic tool such as ENCASE.
B. CP files were acquired, or non-CP files were altered to make them CP [for example, by altering dates.]
C. The files mentioned above were added to the WD HDD 1B16 drive

TASK 1: ANALYZE THE DRIVE PRIOR TO ALTERATION OF EVIDENCE

This would consist of a study of the existing drive for feasibility and content.

ESTIMATED EFFORT:

- **16 Hours by a STAKEHOLDER**
- **16 Hours by a TECHNICAL SUPERVISOR**

TASK 2: ACQUIRE AND PREPARE THE CP FILE CANDIDATES

Selection of CP file candidates would include choosing ones of the appropriate size, other metadata, and conformity with adjoining files.

ESTIMATED EFFORT:

- **24 HOURS by a DATA ENGINEER.**

TASK 3: PERFORM THE ACTUAL CREATION OF THE ALTERED DRIVE

This task consists of actual alteration of their EXIF metadata as needed, deletion of the files they would replace, copying them into the working drive, and then imaging the resulting drive back to the original unit. File date alteration apparently included files outside the 22-file range of the added files, for the appearance of continuity.

ESTIMATED EFFORT:

- **40 HOURS BY A DATA ENGINEER**

PROJECT 2 ESTIMATED TOTAL HOURS:

96 HOURS BY 3 DIFFERENT PARTIES

Discussion

This process subsumes KEY FINDINGS 4, 5, 6, and 7 by Dr. Kiper. His findings 1, 2, and 3 were the subject of the first analysis in this report, above.

A. In KEY FINDING 4, Dr. Kiper reported irregularities of file dates that could not have been the result of any innocent process
B. In KEY FINDING 5, Dr. Kiper reported that irregularities in the EXIF headers of several files exist that could not be the result of any innocent process.
C. In KEY FINDING 6, Dr. Kiper reported that the names of folders were apparently arbitrary, belying their state origins as computer-generated.
D. In KEY FINDING 7, Dr. Kiper reported that the alleged CP were possibly planted and had dates altered to give the appearance they had been sourced from a 2009 backup.

The inclusion of detectable data manipulation errors that were detected by Dr. Kiper and confirmed by myself and by Mr. Abrams raises an obvious question of how such errors were not detected by the person or persons doing the data manipulation prior to their introduction into the FBI's system. Possibilities include lack of quality control, incorrect assumptions that the evidence would never be inspected as thoroughly as it has been by Dr. Kiper, myself, and Mr. Abrams, inadequate calendar time to complete the work efficiently, lack of skill by the full team, or some combination of those items. It seems likely that all four may have played a role.

NOTES ON ESTIMATION

As is well known in Project Management, creating overall estimates for project cost and schedule is extremely challenging:

- Once a task has been identified, that task may be estimated by comparing it with similar tasks from a Body of Knowledge of prior tasks, a process known as Parametric Estimation. Often, of course, the challenge is identifying the specific task.
- Further challenges arise because a task that is new to the individual performing it may take longer than it would for someone who's done it before.
- Still further challenges arise from task-to-task dependencies, the need to stop and start during task completion, and the likelihood that tasks may arise that were not foreseen at the start of the effort.
- The estimates I provided represent my best judgment based on my experience and the information provided to me, subject to the factors described above.

COMMENTARY

It causes me great disappointment to be aware of this situation, as I have the highest regard for law enforcement. I am well aware of the potential significance and ramifications of the analysis I present here, and for obvious reasons, do not make any such statements without significant study. Regrettably, based on the information available to me, and upon significant review, I cannot envision a plausible explanation for the discrepancies noted by Dr. Kiper and reviewed by myself and Mr. Abrams, aside from intentional alteration. This is not a conclusion I am pleased to make.

RESERVATION OF RIGHTS

I reserve the right to amend or augment my opinions and discussions in the above report based on any new information that may come to light, including but not limited to information brought by participants in this case, subsequent research of my own, or information from other reliable and legally proper sources. I further reserve the right to modify the scope of this or other communications I may have in conjunction with this matter, based on information then available.

DISCLAIMER

I am not familiar with the non-technical details of this case, other than having been minimally aware that a case of this nature was in process at the time it was taking place. I have no knowledge of or relationship to any of the participants.

I have provided my credentials in other documents in this case, and I incorporate them into this document by reference.

I am not an attorney, and thus, I have not, and will not, offer opinions of law.

I declare under penalty of perjury, under the laws of California, that the foregoing is true and correct.

Dated: April 27, 2022, at Santa Barbara, California.

WAYNE B. NORRIS