Affidavit of Stacy R Eldridge

State of Nebraska
County of Lancaster

COMES NOW Stacy R Eldridge, 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 dated 9/29/2022
- Summary of Process Findings dated 9/29/2022

Signature: Stacy R Eldridge

Address: 1145 Hackberry St
Bennet, NE 68317

SUBSCRIBED AND SWORN TO before me this 29th day of September, 2022, by Stacy R Eldridge.

Debra A. Grant
NOTARY PUBLIC FOR NEBRASKA

GENERAL NOTARY - State of Nebraska
DEBRA A. GRANT
My Comm. Exp. February 8, 2023

My Commission Expires: 02/08/2023

Stacy R. Eldridge, CFCE, GCFE, LPD
FBI Senior Forensic Examiner (Former)
Digital Forensics and Cybersecurity Expert

September 29, 2022

Summary of Technical Findings

Background

I worked as an employee of the FBI from 2003 to 2012. During that time, I served as an Information Technology Specialist (ITS), a Forensic Examiner (FE) on the Computer Analysis Response Team (CART), a Senior Forensic Examiner (SFE) on CART, and a Digital Evidence Instructor for CART Headquarters.

Within those roles, I conducted over four hundred examinations on over 100 TBs of data, mentored and trained CART Forensic Examiners in Training (FETs), trained and graded Special Agents in the Digital Evidence Extraction Technician (DeXT) program, trained and graded CART FETs on Quality Manuals, Standard Operating Procedures, and evidence processing, and graded CART FE yearly proficiency tests, and trained law enforcement personnel to use Image Scan.

After serving in the FBI, I worked as a Senior Staff Cyber Investigator and Program Manager at General Electric, and Director of Cybersecurity at Lincoln Electric System. I currently provide cybersecurity and digital investigation services.

Review of Evidence

My review and analysis of information included: AccessData Forensic Tool Kit (FTK) Reports and file directory listings produced by the Government of 1B15 (a Lexar CF Card) and 1B16 (a Western Digital Hard Drive), SFE Booth's CART examination notes, drag and drop copy of 1B16 that excluded alleged contraband, a file directory listing of 1B16, court testimony, government exhibits, defense exhibits, government discovery items, search warrants and associated affidavits, chains of custody for 1B15 and 1B16, rule 33 submission submitted by the defense, and reports and portions of work product generated by Dr. J. Richard Kiper as provided to me.

I have examined the data used by Dr. J. Richard Kiper discussed in his "Summary of Technical Findings Report," issued on April 25, 2022. Based on my examination, I agree with the facts as stated in his findings below.

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.

Summary of Findings

The data on the compact flash card (1B15(b)) was altered and manipulated while in the custody of SA Lever of the FBI, who, as a case agent, is not authorized to review this evidence directly. The second FBI examination of the CF Card included additional files not present in the first examination, and some of those files were clearly falsified. Such as four photos matched their alleged backed-up copies on the hard drive by name and modified dates. However, the photos depict a different person in a different location than their counterparts on the hard drive. This would mean that the same camera had to have taken pictures of two different people in two different locations at the same exact time, which is impossible. The most plausible explanation is that a combination of photos and information was added to the CF Card and then manually manipulated to strengthen the relationship between the CF Card and hard drive, and the narrative that all of the photos in question on the hard drive were taken in 2005.

Without a doubt, files, folders, dates, and metadata on the hard drive (1B16) were manipulated. The photos in this case, including the alleged contraband, were planted on the hard drive and appear as if they are part of a backup. Furthermore, several subfolders named after dates/times used the wrong time and point to a human naming the folders after modified dates while forgetting to use a 24-hour clock instead of a 12-hour clock to include the ones containing the alleged contraband. The Government used no other data on the hard drive to establish the validity of the dates of the photos other than information that is easily altered and was indeed deliberately altered, as evident by the remnants of human error left behind. Presently, there is no way to scientifically pinpoint when these alterations on the hard drive were made, but they align with the Government's narrative that the photos were taken in 2005. Moreover, these manipulations appear to be part of an elaborate attempt to manufacture a timeline to support photos taken in 2005, but ultimately a trail of mistakes was left behind.

In this case, it is my expert opinion that the digital evidence was extensively manipulated, and some of this manipulation, specifically regarding the CF card, was executed by a person or persons within the FBI.

Sincerely,

Stacy R. Eldridge, CFCE, GCFE, LPD

Stacy R. Eldridge, CFCE, GCFE, LPD
FBI Senior Forensic Examiner (Former)
Digital Forensics and Cybersecurity Expert

September 29, 2022

Summary of Process Findings

Background

I worked as an employee of the FBI from 2003 to 2012. During that time, I served as an Information Technology Specialist (ITS), a Forensic Examiner (FE) on the Computer Analysis Response Team (CART), a Senior Forensic Examiner (SFE) on CART, and a Digital Evidence Instructor for CART Headquarters.

Within those roles, I conducted over four hundred examinations on over 100 TBs of data, mentored and trained CART Forensic Examiners in Training (FETs), trained and graded Special Agents in the Digital Evidence Extraction Technician (DeXT) program, trained and graded CART FETs on Quality Manuals, Standard Operating Procedures, and evidence processing, and graded CART FE yearly proficiency tests, and trained law enforcement personnel to use Image Scan.

After serving in the FBI, I worked as a Senior Staff Cyber Investigator and Program Manager at General Electric, and Director of Cybersecurity at Lincoln Electric System. I currently provide cybersecurity and digital investigation services.

Review of Evidence

My review and analysis of information included: AccessData Forensic Tool Kit (FTK) Reports and file directory listings produced by the Government of 1B15 (a Lexar CF Card) and 1B16 (a Western Digital Hard Drive), SFE Booth's CART examination notes, drag and drop copy of 1B16 that excluded alleged contraband, a file directory listing of 1B16, court testimony, government exhibits, defense exhibits, Government discovery items, search warrants and associated affidavits, chains of custody for 1B15 and 1B16, rule 33 submission submitted by the defense, and reports and portions of work product generated by Dr. J. Richard Kiper as provided to me.

I have examined the data used by Dr. J. Richard Kiper discussed in his "Summary of Process Findings Report," issued on April 25, 2022. Based on my examination, I agree with the facts as stated in his findings below. I also discovered an additional violation of FBI policy (see V and VI below).

- Receiving unsealed evidence created a broken Chain of Custody.
- The CF Card was accessed by an unauthorized FBI employee.
- The timeline of examination is suspicious.
- Critical evidence was withheld from the defense team.

Summary of Findings

Never in my ten years in the FBI have I seen so many violations of critical FBI policies and procedures applied to key evidence, all in one case, where the CART team included not one but two senior forensic examiners. The fact that these policy violations occurred to digital evidence that, according to my technical analysis, was manipulated while in FBI custody is suspicious and troubling.

Thus, it is my expert opinion if the defense and the Court had been aware of these policy violations, in combination with findings of data manipulation, I do not believe this digital evidence would have been allowed in as evidence during the trial.

I. Unsealed Evidence is Not Normal

The FBI has a policy that applies to all FBI personnel that dictates how digital evidence is to be handled, preserved, and examined. First, all digital evidence is to be secured and sealed to prevent loss, damage, and harm; this ultimately protects the integrity of the device and its data. When the integrity of evidence is not protected, any information gleaned from it could be called into question because anything could have happened to it while it was unsealed. A chain of custody is used in conjunction with this policy to protect the integrity of evidence and document who was responsible and accountable for its protection during that period.

During my time in the FBI, I was trained that digital evidence must always be received sealed, and if it was not, then it should be documented in exam notes, and I trained CART personnel the same. I cannot recall a time in over four hundred exams in the FBI when I received unsealed evidence for routine examination. In this case, the Government downplayed the severity of the fact that the CF Card was not sealed when it was given to CART for examination in June of 2019, nor was it documented in the exam notes.

II. Unauthorized and Prohibited Review of Original Digital Evidence

The same FBI policy also dictates who can review original digital evidence and in what order. Original digital evidence is to be given to CART personnel for examination first, and only after that can other personnel review a copy (not the original). This case is especially troubling because at least two persons in the FBI, SA Maegan Rees and SA Michael Lever, conducted unauthorized and prohibited reviews of the CF Card before the evidence was given to CART, as documented on the Chain of Custody. Even more troubling, I found evidence that the data on the CF Card was altered while in possession of SA Lever. Not only did unauthorized personnel review original digital evidence, but they also did so without a write blocker. They did not protect the integrity of the data. And in fact, they altered some of the data on it. Any time digital evidence is reviewed, it must be documented. I have not received any reports written by SA Rees and SA Lever documenting their unauthorized reviews of original digital evidence.

III. Untimely Examination of the CF Card

All of the evidence in the case except for 1B15 was submitted to CART for examination on 8/18/2018. Even though SA Rees and SA Lever had reviewed 1B15 in July and September of 2018, the CF Card was not submitted to CART until 2/22/2019. 2/22/2019 happened to be the same day a new search warrant was issued authorizing the search for child pornography on the hard drive only. Since SA Rees and SA Lever reviewed the contents of 1B15 five months earlier, one can logically assume the CF Card was identified at that time and should have been submitted to CART just like the rest of the digital evidence. I have trouble identifying an innocent explanation for this breach of protocol. Thus, I am left with the questions: Why didn't either Special Agent submit the CF Card to CART sooner? Did their unauthorized reviews not find any evidence pertaining to the search warrant?

IV. Unauthorized and Prohibited Re-Examination of Original Digital Evidence

The FBI policy only allows one examination of original digital evidence. Based on the FTK Report, the first FBI exam of the CF Card was completed on 4/11/2019 by SFE Stephen Flatley. An unauthorized re-examination of the CF Card was started at the tail end of the trial on 6/10/2019, as documented in SFE Brian Booth's exam notes. SFE Booth documented that the process to gain approval for a re-examination was not followed. Furthermore, there was no need for a re-examination because SFE Booth could have obtained access to the case on the CART Storage Area Network, a backed-up copy of the case from evidence control, or asked SFE Flatley for his working copy. After SFE Flatley completed the first exam, he provided the CF Card to SA Elliot McGinnis, who held it over the weekend, and then provided it to SA Christopher Mills, who had it for approximately seven hours and finally provided it to SFE Booth. It took four days to get the CF Card from one CART examiner to another who presumably worked in the same physical location. SFE Booth completed his re-examination on 6/11/19 with wildly different results. I have difficulty seeing an innocent explanation for this when taken together with the CF Card changing hands three times in four days before arriving in an unsealed bag to SFE Booth. I am left without an innocent answer based on the information provided to the defense for the following question: How could two highly trained Senior Forensic Examiners in CART have such drastically different results?

CART Examiners are allowed to analyze the processed evidence repeatedly. Any additional analysis only requires additional notes and reporting. This is a frequent occurrence during an investigation and trial preparation. While in the FBI, I conducted additional analysis numerous times without imaging and processing the evidence again. On occasion, when the first CART Examiner is unavailable, another CART Examiner can review the CART notes, CART reports, and open the FTK case to conduct additional analysis. The evidence doesn't need to be imaged or processed again. Thus, one must ask, why did SFE Booth process the evidence again when it was not required? FBI policy specifically prohibits re-examination to protect the integrity of the evidence. In this instance, it seems that integrity was again not protected, as evidenced by four photos on the CF Card that matched their alleged backed-up copies on the hard drive by name and modified dates. However, the photos depict a different person in a different location than their counterparts on the hard drive. The most plausible explanation I can deduce is that the violations in FBI evidence-handling policy resulted in the alteration of the evidence.

V. Providing Original Digital Evidence to the US Attorney's Office is Prohibited

Per FBI policy, only an image or working copy of original digital evidence may be provided to the USAO. In this case, I found evidence of the CF Card, original digital evidence, being provided to the USAO. On 9/27/2018, AUSA Tanya Hajjar told the Court, "I think one of those was like 8 Hale camera, for example. We just pulled out the pictures out and gave them [the defense] everything." The 8 Hale camera she is referring to is 1B15. How was the USAO able to pull everything off of the CF Card? One can only conclude they were given the original digital evidence to do this since CART had not been given this piece of evidence yet.

The Government's letter regarding discovery is dated 9/25/2018 and describes the photos pulled off from 1B15 as VDM_NXIVM00005028-VDM_NXIVM00005130. These items were provided to the defense in two PDF files. Both of these PDF files were created on 9/21/2018 and authored by TCarby. It's logical to assume that TCarby is Terri Carby, a paralegal specialist in the USAO, as documented in a press release dated 7/12/2022 regarding the Attorney General's awards.

Again, these files were created nearly five months before the CF Card was provided to CART for examination. It is unknown how TCarby obtained the files to include in discovery, but the chain of custody for the CF Card indicates SA Lever had custody of the CF Card on the date TCarby created the PDF files.

In my ten years of experience at the FBI, I am unaware of a single case where the USAO office handled digital evidence before the FBI. I'm left with the question, why did the USAO's office handle the CF Card in September 2018 when it was only an 'accidental' discovery five months later that demonstrated the significance of this piece of evidence?

VI. Unauthorized and Prohibited Examination by an Outside Agency

A forensic tool was used to produce the photos included as items VDM_NXIVM00005028-VDM_NXIVM00005130 (as noted above), including deleted and carved files. A forensic tool must be used to recover deleted and carved files; this process is considered an examination in the FBI. This is significant because not only is it against FBI policy, the FBI did not conduct the first examination of the CF Card. It is unknown who conducted the examination, their training, what procedures were followed to create these results, or what steps were taken to protect the CF Card's integrity.

It's also important to note that these files provided by the Government as part of the discovery visually appeared to match only the results of the FTK Report dated 4/11/2019 and not the 6/11/2019 FTK Report. This further calls into question the reliability of the information present on the CF Card on 6/10/2019 and causes one to wonder what was done to the CF Card between the first and second FBI examinations.

VII. The Unreliability of EXIF Data

In this case, EXIF data from the CF card and the hard drive played a central role in the Government's narrative used to convict, and SFE Flatley and SFE Booth examined the CF card. In the past, SFE Flatley has testified on EXIF data's reliability. In a different trial, SFE Flatley

testified EXIF data was easily altered and unreliable. In this trial, SFE Booth testified to the opposite and that EXIF data was difficult to alter and highly reliable. In my experience, personally and professionally, it is my expert opinion that EXIF is easily modified by a person knowledgeable in computers without special software, and EXIF data by itself is unreliable.

VIII. Critical Evidence was withheld from the defense team

The defense was not provided with an image (a forensic copy) of the CF Card created by SFE Flatley or by SFE Booth. Nor were they provided any logs and file directory listings that accompany the images. The FTK processing logs from the exams conducted by SFE Flatley or SFE Booth were not provided. Only the PDF version of the FTK Report created by SFE Booth was provided, not the report's HTML version. This is significant because some hyperlinked files were not included in the PDF version of the report. I have not received any of these items either. Without these critical pieces of information, the defense and the jury were not provided with all of the information in this matter.

Conclusion

Based on my FBI experience and knowledge of FBI policies and procedures, it is my expert opinion that personnel in the FBI violated several critical FBI policies, procedures, and best practices when handling digital evidence.

Sincerely,

Stacy R. Eldridge, CFCE, GCFE, LPD