EXHIBIT B

United States of America v. Keith Raniere, et al	IN THE UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK CRIMINAL DOCKET FOR CASE #: 1:18-cr-00204-NGG-VMS.	AFFIDAVIT OF Steven M. Abrams, J.D., M.S. In Support of the Summary of Technical Findings by J. Richard Kiper, PhD, PMP

PERSONALLY APPEARED BEFORE ME, the undersigned, who, being duly sworn, deposes and states the following:

1. My Name is Steven Marc Abrams. I am a licensed Attorney and Counselor at Law, in good standing, in South Carolina, Washington, DC, and New York. I am a retired State Constable in South Carolina. My field of concentration is digital forensics. I have assisted municipal, county, state, and federal law enforcement agencies and the US Department of Defense and the Department of State with digital forensics investigations for over three decades. For 11 years, from 2008 until 2019, until my retirement I held a law enforcement commission from the Governor of South Carolina at the request of the United States Secret Service. My office address is 1154 Holly Bend Drive, Mount Pleasant, South Carolina 29466. My office phone number is (843) 216-1100. My full credentials are included in my CV which is appended to this affidavit.
2. From 2002 until 2014, I taught digital forensics classes to police and military organizations around the world using Accessdata FTK. I am familiar with the tool, first being certified in its use at the North Carolina Justice Academy (NC state police academy) in 2002. I have used FTK regularly for nearly 20 years.
3. In my career as a digital forensics' examiner working closely with law enforcement I have never observed, or examined creditable evidence of, a purposeful mishandling of digital evidence by any law enforcement agency, nor made any report of the same. I have never previously observed or reported evidence tampering by law enforcement.
4. I was retained by counsel and signed onto the Protective Order on 05/21/21 to review certain digital forensics evidence used in the trial of Keith Raniere *et al*. In the process of fulfilling that mission I reviewed (1) relevant portions of trial transcript,(2) the written statements of other experts for the defense, (3) the government's digital forensic evidence

provided to me by Mr. Raniere's defense counsel pursuant to the protective order, and (4) have conducted my own experiments using a Canon EOS 20D camera similar to the one that was used to create certain digital photographic material and related filesystem artifacts that are relevant to the government's case against Mr. Raniere. I have also used various digital forensics tools from AccessData, BlackBag Technologies, and CelleBrite to review portions of the Government's evidence that were provided to me.

5. This affidavit concerns my review of the April25, 2022, "Summary of Technical Findings" by J. Richard Kiper, Ph.D., PMP. Dr. Kiper, is a retired FBI Special Agent and Forensic Examiner. Dr. Kiper reviewed forensic evidence and trial testimony related to certain digital photographs, some of which the government alleged were contraband. Crucial to this claim by the government was an accurate fixing of the date the photographs were taken, and as with all evidence, proof that the photographic evidence in question was reliable and authentic. The way the photographic material was handled by the FBI, who performed the forensic examination of the evidence for use at trial, is a crucial "gatekeeper" threshold question for any forensic evidence that is destined for use in a criminal trial. Dr. Kiper further addressed the FBI's evidence handling in this matter in his April 25, 2022, "Summary of Process Findings." While I have worked parallel investigations with the FBI, I have never worked for the Bureau, so I don't have direct knowledge of FBI policies and procedures and have therefore taken this document at face value and used it to provide further understanding of Dr. Kiper's Summary of Technical Findings.

6. In his Summary of Technical Findings Dr. Kiper noted seven key findings that lead him to conclude the evidence was manually altered while in the custody of the FBI, and these manual alterations taken together lead him to conclude the FBI tampered with key evidence during the months prior to Mr. Raniere's trial. After a careful review of the

evidence and the work done by Dr. Kiper, I agree that the data and forensic artifacts cited by Dr. Kiper are genuine. Further, it saddens me to concur that the only logical conclusion to be drawn by any reasonable person for the set of forensic artifacts demonstrated by Dr. Kiper is that a manual alteration of the digital photographic and filesystem evidence, and an unsuccessful attempt to cover that manual alteration, occurred while the evidence was in the custody of the FBI.

Finding 1.

7. Dr. Kiper's first finding deals with certain photos found both on a CF card from a Canon 20D camera and on a Western Digital Hard drive ("WD HDD") that were two key sources of evidence relied on by the Government. The Government needed to show that the photos in question were created and possessed by Defendant. However, the origin of the photos on the WD hard drive was uncertain. Throughout the case the government alleged that the Canon 20D camera belonged to Defendant and thus they could argue that any photos taken by that camera and found on a CF media card that was associated with that camera, were likely taken and possessed by Defendant.

8. the government made two different forensic images of the CF card associated with the 20D camera. This second image of the CF card is crucial to Dr. Kiper's first and second finding. On the second image of the CF card, and only on the second image, there appeared a set of files whose filenames and modified dates were identical to the digital photos found on the WD hard drive (WD HDD) that were in the same range as the alleged contraband, all purportedly taken by the same camera. Because the filenames and dates matched between the backup located on the WD HDD and CF card, it appeared that the contraband photos also came from the CF card that was in the camera that was alleged to be used by Defendant, even though none of the contraband, or remnants, were found

on the CF card. However, forensic analysis of the files from both the CF card and the WD hard drive revealed that although containing the same filenames and modified dates, they contained different MD5 hashes, and thus different contents. MD5 hash codes are large prime numbers that are computed from every byte of data in a file, and thus uniquely identify files by every bit of data contained within them. Any alterations to a file will change the MD5 hash code value for the file. Thus, hash codes, such as MD5, are used to quickly determine to near 100% accuracy if the data contained within two digital files is the same or different. In this case two sets of files that appeared outwardly to be the same, one set on the WD HDD backup and the other on the CF card from the camera, are in fact completely different. Dr. Kiper concluded in his first finding that it was not possible for these two unrelated sets of files to have the same filenames and dates, down to the exact second, unless someone intentionally set it up to look that way to create the appearance of a stronger connection between the contents of the CF card and a backup contained on the WD hard drive. I agree.

Finding #2.

9. Dr. Kiper's second finding deals with the manual addition of digital photos onto the Compact Flash (CF) card used as digital media in a Canon 20D camera which held the photos that became the Government's key evidence in this case. These are the same suspicious digital photos that were discussed above in Finding 1. The trial record indicates that the FBI made two different forensic images of the CF card associated with the Canon 20D camera. The initial forensic image was made in April 2019 and a second forensic image was made in June 2019. The forensic image made in June contained additional files which the filenames indicate are digital photos (discussed in Finding 1) not contained

in the forensic image made in April 2019. That the contents of the two forensic images were not identical is significant and troubling. Forensic imaging is based on the foundational principle that no matter how many different examiners make an image of a given device that the forensic image produced by any competent examiner using any valid imaging tool will contain exactly the same data (e.g., set of contents) as the image produced by any other competent examiner from that common device. Any differences in the data between the forensic images, no matter how minor, is de facto proof that the contents of the device being imaged changed from the time the image was first made to when the subsequent image was made. In this case, alarmingly, the second image made in June 2019 contained additional files not contained in the original forensic image made in April 2019.

Upon determining that the two forensic images of the CF card contain different evidence a neutral investigator must ask if there could be any innocent explanation for how these two images of the same device contained different contents? In the past I have seen AccessData FTK under carefully controlled laboratory conditions produce different numbers of files from the same e01 forensic image file when running under different version of Microsoft Windows. That anomaly does not seem to apply here, the two forensic images contain different evidence. Dr. Kiper has identified specifically the files that were added to the second forensic image. Dr. Kiper explored the origins of these new files that appeared in the June 2019 forensic image of the CF card in his finding #1. He also determined that not a single viewable photo was able to be carved out of these new files despite filenames and system dates that made them appear to be specific digital photos that also appeared on the Western Digital hard disk drive ("WD HDD") that was another source of evidence used by the FBI in its investigation. Dr. Kiper noted that despite

the fille names and system dates of the new files on the CF card being identical to photos appearing on the WD HDD, none of the MD5 hashes of the new files appearing on the CF card matched the MD5 hashes for similarly named files on the WD HDD. Thus, they were not the same files, only the names and dates were identical, not the contents. He surmises that someone created the new evidence on the CF card with similar names and dates to files on the WD HDD to make the link appear stronger between the evidence on the WD HDD (from an uncertain providence) and the evidence from the CF card that the government contended was linked to Keith Raniere. I have reviewed Dr. Kiper's analysis, and his work is conclusive to a scientific certainty. **Based on Dr. Kiper's thorough analysis, I sadly concur that the only reasonable explanation of the additional files appearing in the FTK listing of files on the CF card from the June 2019 forensic image is that additional evidence was manually added to the CF card between April 2019 and June 2019 while the CF card was in FBI custody and that was likely done to make evidence found on the WD HDD appear to be linked to the CF card, which the government contended was linked to Mr. Raniere.**

Finding #3.

10. Dr. Kiper's third finding is that the filesystem access date metadata was overwritten on 9/19/2018. I agree. This sort of mishandling of digital evidence is common among lay people, I regularly observe attorneys mishandle their client's evidence produced in discovery in this manner, but this sort of mishandling of evidence is unexpected from the FBI. This alteration of the access date metadata proves to a scientific certainty that the CF card was inspected without using a write protect device or write blocking software on the computer used to review the data on the CF card. This is either a rookie mistake, or

a purposeful act of digital sabotage. Either way **this crucial filesystem metadata was spoliated while the CF card was in FBI custody.**

Finding #4.

11. Dr. Kiper's fourth finding is "Dates of photos on the hard drive were altered through manual intervention." This finding is based on a comparison of the modified date metadata of certain jpeg files on the CF storage card from the Canon camera and the metadata on the same files in a backup copy on a computer hard drive. Every jpeg photo contains two types of metadata, filesystem metadata, common to all computer files, and EXIF metadata that is embedded within the JPEG photo itself. Both types of metadata preserve timestamp information associated with the photo. In a perfect world one would expect there to be a logical relationship between the EXIF timestamps from images on the camera CF card and the modified filesystem timestamp from the image files on the hard drive. In this case, the timestamps start out being 1 hour apart, with the hard drive copy being one hour behind the camera media. Then on 10/30/2005 when daylight saving time ends it appears the computer falls back and is two (2) hours behind the camera, which is not programmed to handle daylight savings time. This might be what one would expect to see happen at the end of daylight savings time. However, unexpectedly by the afternoon of 10/30/2005 when the next photo, IMG_138.jpg, is taken the clocks in the computer and camera are in synchrony and there is no difference between the timestamps in the computer and camera. We do not know when the photos were copied to the hard drive, but the timestamp differences would not have happened in real time, as the data on the CF card was not written to the camera until some later time. Given that the camera was not programmed to make changes to its time settings as a result of Daylight Savings Time,

and used a FAT 16 filesystem on the CF card two things are known to be true: First, the camera was incapable in making any automatic changes to its time settings and requires a manual setting of the time by the camera user for any time settings observed in the data produced by the camera. Second, given the FAT 16 file system one would expect the filesystem modified timestamp on the CF card to be copied exactly, without any adjustments for time zone or Daylight Savings Time, on any copies of the files copied to a computer or external media. There is a possibility that Windows may have been set to automatically adjust for Daylight Savings Time, and that might account for some of the one hour shifts of the clock in this data. This would not account for a two-hour shift seen in one day, as for example on 10/30/2005. Thus, it would appear that these odd shifts in timestamps could not be accounted for by any software mediated process, and at least some of these time shifts resulting in a two hour difference were more likely the result of manual intervention. **I agree with Dr. Kiper's Fourth finding. The filesystem modified timestamps on this evidence are highly suspect and unreliable. The most plausible explanation for the pattern of time differences observed in this data, especially those that are two hours different, is manual manipulation of the timestamps.**

Finding 5.

12. Dr. Kiper's fifth finding deals with IMG_0175.jpg, and the curious metadata on and embedded within that photo. The first red flag in this photo is in the EXIF data which indicates that the image was modified using "Photoshop Adobe Elements 3.0." From this information alone we know that someone modified this photo. It is not in its original state as captured by the camera. Next, the filesystem modified timestamp on the CF card copy of the image matches the filesystem modified timestamp on the copy of this image on the hard drive. This is another red flag, as one would

expect that if one edited the photo and resaved it using Photoshop that the modified timestamp should reflect the time of the editing, not the time the photo was taken and written to the CF card by the camera. Thus, one must conclude there was an attempt to conceal the fact that the photo was altered on the hard drive by manipulating the filesystem modified timestamp on the computer hard drive to match the filesystem modified timestamp on the CF card. I therefore agree with Dr. Kiper that this digital photograph, IMG_0175.jpg, was manually modified ("Photoshopped") using Photoshop Adobe Elements 3.0, and the fact that the filesystem modified timestamp was not changed to reflect the editing with Photoshop is evidence for Dr, Kiper and me, that someone likely manually modified the filesystem timestamp to conceal the fact the image was edited with Photoshop. The only reason we know that this file (IMG_0175.jpg) was edited with photoshop is that this is the only photo that still has the CreatorTool field intact in the EXIF header. As Dr. Kiper points out this probably was an oversight by whomever did the editing. I think that Dr. Kiper is likely correct.

Finding #6.

13. Dr. Kiper's sixth finding concerns the folder names of the folders that contain the alleged contraband photos. The folder names appear to contain an embedded computer-generated time and date "timestamp". This embedded timestamp was crucial evidence for the Government at trial as it was the only basis the Government had to "independently" determine the date when the alleged contraband photos were taken, apart from easily editable EXIF dates. A careful review of this embedded timestamp data by several experts for the defense all conclude that this data is not reliable and at least some of this data was likely assembled manually in an attempt to appear to have been generated automatically

by a computer program to add an appearance of credibility to the timestamps. In finding #4 it was determined that Adobe Photoshop Elements 3.0 was used to edit at least one of the photos. This program can also be used to import photos from a camera. When the Adobe Photoshop Elements software is used to import photos from a camera it can create a timestamped folder with an embedded timestamp. It is important to note that that the timestamp which is embedded in the filename corresponds to the date the images are imported, not when they were taken. So even if this was the means of creating the timestamped folder names, the timestamps would not accurately reflect when the photos were created, as was claimed by the Government.

14. Upon careful review of the folder names and the files copied into each folder it appears impossible that a program imported the files and created the folder names with the embedded timestamps as the Government claimed had happened, and therefore had to have been manually manipulated. For example, the folders "2005-10-19-0727-57" and "2005-10-19-0727-59" would have been created only two seconds apart, yet the earlier folder ending -57 contains nine photos, and the later folder ending -59 contains 11 photos. It seems unlikely, given how slow the Canon D20 with its CF media was to upload photos, that these nine photos could be copied in only two seconds. Also, the sequence of photos in these folders doesn't make any sense if one assumes a program created the folders and copied the photos into them. The earlier folder (ending -57) contains images numbered 0090 to 0098, while the later folder (ending -59) contains images numbered 0079 to 0089. It seems very unlikely that a program would copy the photos off the CF media out of order. This is outside my experience as an avid amateur photographer familiar with all the leading photo software packages.

15. The only plausible explanation I can think of for this evidence is that someone manually created these folder names as part of a scheme to have a legitimate appearing means of proving when the alleged contraband images within the folders were taken. This was necessary as there was no reliable means of dating the alleged contraband photos from the computer filesystem metadata which had been corrupted prior to the FBI's examination of the computer, or the camera date which was also unreliable. During the trial the FBI examiner and the prosecutor both used the likely fictitious timestamp embedded in the folder names as a means of establishing a date for the alleged contraband photos contained within the folders and told the jury they knew when the photos were taken based on the dates in the folder names. This is totally unscientific and misleading at best. **Based on the totality of the evidence, the way in which the government relied on these embedded timestamps at trial, to establish a date certain that the alleged contraband photos were taken, was knowingly and purposely misleading to both the Court and the Jury. I agree with Dr. Kiper's conclusion regarding his finding #6.**

Finding #7.

16. Dr. Kiper's seventh finding deals with an apparent attempt to plant incriminating evidence in a backup on the hard drive. This planted evidence consists of a selective (manual) backup containing the alleged contraband images. The planted backup appears to be part of a series of backups performed on 03/30/2009. Each of the backups in the series contains the name of the computer model and the backup date embedded within the filename for the backup. It appears the filenames for each backup in the series was automatically generated from the computer name and the date the backup was made. The

files in the first two backups have filesystem metadata indicating they were copied into the backup on 3/30/2009, the date embedded in the filenames for the backups. However, this is not true for the files contained in the third (suspect) backup. Based on the filesystem metadata for the files within the third backup, it appears that someone manually generated the filename from the computer model and a misleading timestamp to make the backup appear to be part of the series of backups from 03/30/2009. This leads us to conclude there was an attempt to create this selective backup and make it appear to be part of a series of automatic backups that were made to the hard drive on 3/30/2009. This misleading filename and the fact that the alleged contraband images were cherry picked to be included in the backup strongly suggests that someone created this backup and placed it on the hard drive to plant incriminating evidence while attempting to conceal the fact the evidence was being planted in this manner. I agree with Dr. Kiper's interpretation of this evidence.

17. In addition to concurring with Dr. Kiper's observations and conclusions, I have a few additional observations that I made in my review of this evidence that I would like to include in this affidavit. In my reading of the trial transcript of FBI examiner Booth, I was struck by two points that he made and that were then echoed by the prosecution that he knew or should have known after his many years as an FBI Digital Forensics examiner to be false or likely false. To wit:

18. First, Booth's insistence that the dates embedded in the EXIF headers of the evidence photos were known to be reliable, even in the absence of any extrinsic evidence, because EXIF data was so hard to alter is misleading at best. A cursory search of the Internet would inform Mr. Booth and the Prosecution that there are many readily available inexpensive

(or free) software products that facilitate changing EXIF data of the kind that Booth insisted was not easy to change. Additionally, the Adobe Photoshop Elements 3.0 software that was used to alter at least one evidence photo (see Finding 4 above.) and to possibly import some of the images discussed in Finding #5 above, has a built-in feature that allows one to alter the EXIF timestamps. Since we already know that someone was manipulating the photographic evidence in this case with Photoshop Elements software, we know that same person had a tool that was designed to easily change the EXIF timestamps at will. Thus, Booth was either negligent or perjurious in his insistence that the EXIF timestamp data embedded in the photographic evidence used at trial was hard to change because it "was designed that way."

19. Second, Booth's testimony that it was not unusual to receive evidence in an unsealed evidence bag is similarly misleading and similarly seems to be his position at trial because it helped bolster the crucial evidence that the Government needed to rely on despite its dubious nature. While I have never worked for the FBI, I was sworn law enforcement for over 11 years at the request of the US Secret Service field offices in South Carolina. In all I worked digital forensics cases for over two decades with Municipal, State and Federal law enforcement agencies (including the FBI and US Secret Service) and with military units of the United States and friendly foreign countries. During all that time it was always my experience that evidence was placed into a sealed evidence bag and a chain of custody started by the agent / officer who initially collected the evidence. In hundreds of cases I was the initial officer who collected the evidence and began the chain of custody. I always placed the evidence into an evidence bag and affixed a tamper evident seal before passing the evidence on in the chain of custody as I and every other classmate of mine at the North Carolina Criminal Justice Academy was trained to do. I was taught that

any evidence that arrived from further down the chain of custody in an unsealed state should be considered to be outside a proper chain of custody and not usable in a criminal matter. This is not just my experience in all the agencies for whom I worked, but also what Dr. Kiper reported from his knowledge of how things worked at the FBI. Not only would Examiner Booth have known that unsealed evidence was unusual and suspect, the prosecutor also would have been well aware of this issue, and wary that it could form the basis of a successful motion by the defense for exclusion of the evidence. Booth's insistence that the unsealed evidence in this case was not unusual was nothing other than a gratuitous false statement meant to preserve evidence that rightly should have been found to be inadmissible.

FURTHER THE AFFIANT SAYETH NOT!

Steven M. Abrams

Steven Marc Abrams, J.D., M.S.

SWORN TO AND SUBSCRIBED BEFORE ME THIS
26, DAY OF April, 2022.

Amanda Maiello

NOTARY PUBLIC FOR SOUTH CAROLINA
MY COMMISSION EXPIRES: March 18, 2024

EXHIBIT B1

APPENDIX A.

Steven M. Abrams, J.D., M.S.
Curriculum Vitae

Steven M. Abrams, J.D., M.S.
Attorney, Digital Forensics Examiner and Instructor
1154 Holly Bend Drive
Mount Pleasant, SC 29466
843-216-1100
Steve@AbramsForensics.com

Curriculum Vitae

My key practice areas are Computer Forensics, e-Discovery, and Computer Law.

Education

2016 -Techno Security 2016, Computer Forensics Training Seminar, Myrtle Beach, SC, June 5-8, 2016

2014 -Georgia Bureau of Investigations, Internet Evidence Finder Forensics Training, Decatur, Georgia, February 2014

2013 -Techno Security 2013, Computer Forensics Training Seminar, Myrtle Beach, SC, June 2-5, 2013

2012 -Techno Security 2012, Computer Forensics Training Seminar, Myrtle Beach, SC, June 3-6, 2012

2011 -November 9-12: EnCase 7 Training, Salt Lake City, UT
-November 6 – 9: Paraben Forensics Innovations Conference, Park City, UT
- South Carolina Assoc. of Legal Investigators (SCALI) Annual Training Seminar, May 2011
- April 7, 2011: SC Electronic Crime Task Force Quarterly Meeting and Training

2010 -Techno Security 2010, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2010

2009 - Cellebrite Mobile Device Forensics Certification (CCMDE), SEMAR, Mexico City, Mexico
-SCALI Annual Training Seminar, May 2009

2008 - South Carolina Basic Constable Training, Tri-County Technical College / SC Criminal Justice Academy, October – November 2008
- Commissioned as a South Carolina State Constable (LEO) on November 20, 2008.
- Techno Security 2008, Computer Forensics Training Seminar, Myrtle Beach, SC, June

2007 - Charleston School of Law, Charleston, SC, Juris Doctor (J.D. - Magna Cum Laude)

- GMU2007 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2007 (40 CEU HTCIA)
- Techno Security 2007, Computer Forensics Training Seminar, Myrtle Beach, SC, June

2006 - University of Aberdeen, School of Law, Kings College, Old Aberdeen, Scotland in collaboration with the University of Baltimore Law School Summer Law Program in Comparative Criminal Procedure and UK Business Entities & Taxation
- Techno Security 2006, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2006

2005 - SCALI Annual Training Seminar, May 2005
- SCALI Fall Training Seminar, October 2005

2004 - Access Data Advanced Windows Forensics, June 23-25, 2004, New York City. (24 Credit Hours)
- SCALI Annual Training Seminar, May 2004 (10 CEU)

2003 - GMU2003 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, George Mason University, Fairfax, VA. Aug.2003, (40 CEU HTCIA)
- Techno Security 2003, Computer Forensics and Security Conference (24 CEU)
- SCALI Annual Training Seminar & PI Training Seminar (16 CEU SLED)

2002 - SCALI Annual & Fall Training Seminars (16 CEU SLED)
- GMU2002 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2002, (40 CEU HTCIA)
- Access Data Computer Forensic Boot Camp, North Carolina Justice Academy, Edneyville, NC (24 CEU)

1992-1994 Microsoft Internet Developer Workshops NY, NY

1992-1993 Novell NetWare CNE Training, IBM Skills Discovery, Jericho NY

1984-1985 Microcomputer and Electronics Engineering, Hofstra University, Hempstead NY

1982-1983 Ph.D. Studies, Faculty Fellowship, Columbia University, Graduate School of Arts & Sciences

1981-1982 Columbia University, College of Physicians & Surgeons, Master of Science (M.S.)

1977-1981 Allegheny College, Meadville PA, Bachelor of Arts (B.A.) (Psychology - Computer Science)

Professional Licenses

Current

Licensed Attorney in South Carolina
Licensed Attorney in District of Columbia
Licensed Attorney and Counselor at Law in New York

Previous

Licensed as a Private Investigator in South Carolina and New York (2002-2008), South Carolina State Constable (Sworn, 2008-2019).

Experience (Selected)

2016 – Present, Senior Attorney, Abrams Cyber Law & Forensics, LLC. Mount Pleasant, SC 29466. Concentration on Electronic Privacy and Defamation Cases, Electronic Discovery, and Digital Forensics.

2018 - Continuing Legal Education Instructor, ***Electronic Privacy Violations during Divorce: Legal and Ethical Guidelines for Family Law Practitioners,*** SC Bar, Columbia SC (February 21, 2018).

2016 – Continuing Legal Education Instructor, ***Smartphones as evidence for Personal Injury Cases***, NBI, Charleston SC (December 8, 2016).

2011 – 2016 Sole Practitioner Abrams Law Firm, PC. Mount Pleasant, SC 29466

2011 - Digital Forensics Instructor / Investigator, H-11 Digital Forensics / United States Embassy, Tirane, Albania.

2010 – Facilitator, Instructor, Annual In-Service Legals and CDV Training (SLED), Lowcountry Constable Association.

2009 – Speaker, South Carolina Association for Justice, Hilton Head, SC (August 6, 2009) Topic: Civil Discovery of E-mails after *O'Grady*

2009 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Faculty, SC Bar Convention – Family Law Section CLE

2008 – 2011 Shareholder, Abrams Millonzi Law Firm, P.C., Mount Pleasant, SC 29464

2007 - Presenter, "E-Discovery: Definition, FRCP Changes and Application CLE",NBI, Charlotte, NC, December 19, 2007

2007 - Digital Forensics Instructor/Investigator, H-11 Digital Forensics, United States Embassy, Mexico City, Mexico

2007 - Presenter, "Civil to Criminal: Collaborative Computer Forensics Investigations between PIs and Law Enforcement",GMU2007, August 9th & 10th, 2007

2007 - Presenter – "A South Carolina Lawyer's Roadmap to Navigating the New Federal E-Discovery Rules," The South Carolina Bar (CLE Division), April 13, 2007.

2006 - Presenter – "Typical Internet Sexual Activity and its Detection", Family Law CLE, The South Carolina Bar (CLE Division), November 2006.

2006 - Instructor, "3-day Hands-on Computer Forensics Workshop", Trident Technical College, N. Charleston, SC, CLE accredited by The South Carolina Bar, January 2006.

2005 - Lecturer, "Computer Forensic Introduction", Trident Technical College, CLE accredited by South Carolina Bar and CEU / In-Service hours for PIs / LE by SLED.

2001 - Present Steve Abrams & Company, Ltd. (dba Abrams Computer Forensics)
Licensed Private Investigator, Computer Forensics Examiner

1998 - 2001 Steve Abrams & Company, Ltd. Mt. Pleasant, SC, President

1996 - Democratic National Committee, Instructor - Southeast and Northeast Regional Schools for Congressional Campaign Managers.

1995 – 1999 Direct Marketers of Charleston Mt Pleasant, SC, Partner
Co-owner of Political Database Marketing Company and full service political print shop.

1994 - 1995 The Software Studio Mt Pleasant, SC, Owner
Owner of software development company that developed database applications for the Newspaper publishing industry.

1992-1993 Town of North Hempstead, Manhasset, NY, Deputy Commissioner of Finance
.

1986 - 1992 Digitron Telecommunications, Inc., Huntington, NY, Director of R&D

1984 - 1986 Computer Associates International., Islandia, NY, Senior Systems Programmer

1983 Contel Information Systems Division. Great Neck NY, Software Engineer
(Developed the first Network Forensics Applications for the DoD

Recent Publications

Steven M. Abrams, Knowledge of Computer Forensics Is Becoming Essential for Attorneys in the Information Age, 75 N.Y. St. B. Assn. J. 8, 15 (Feb. 2003).

Steven M. Abrams, Knowledge of Computer Forensics, Essential for 21st Century Private Investigators, 16 PI Mag. 46, 59 (October 2003).

Professional Awards & Honors

2008 – Member, SLED Ad Hoc Committee on Computer Forensics

2007 – CALI Excellence for the Future Award, Aviation Law, Charleston School of Law, Fall 2006

- CALI Excellence for the Future Award, Interviewing, Counseling & Negotiation, Charleston School of Law, Fall 2006

- CALI Excellence for the Future Award, Insurance Law, Charleston School of Law, Fall 2006

_ Dean's List, Charleston School of Law, Fall 2006, Spring 2007.

2004 - "2004 SCALI Investigator of the Year"

2003 - Member, SLED Private Investigations Business Advisory Committee

Professional Associations

Member, Institute of Electrical and Electronics Engineers - IEEE
Member, Lowcountry Constables Association - LCA

Bar Association Memberships

Admitted to practice in **South Carolina, District of Columbia, and New York**.

Compensation

I receive $350 per hour, plus mileage, travel and lodging expenses, for all Computer Forensics services and for depositions and trial testimony.

Previous Expert Testimony

I have completed over 1200 computer forensics investigations, the overwhelming majority of cases were settled and did not require me to testify.

South Carolina cases in which I was qualified in court as an expert are:

Hillburn v. Hillburn, (2001-DR-08-2354);
Smith v. Smith, (2001-DR-22-212);
Natale v. Natale, (2003-DR-10-775)
Berda v. Berda, (2003-DR-10-1899*)*;
Murphy v. Murphy (2004-DR-10-1510) and
Overstolz v. Fountain of Youth Wellness Centers LLC (2003-CP-10-000761).
Gitter v. Gitter (2008-DR-10-2865)
Ricigliano v. Ricigliano, (2009-DR-18-0102)
Edwards v Junevicus, (2010-DR-10-4736)
BTM Machinery Inc. v. Michael J. Finley (2013-CP-10-4366)
Cherry v Cherry (2014-DR-10-95)
Whitfield v. Schimpf and Sweetgrass Plastic Surgery, LLC (Case No. 2017-CP-10-2758)

I was qualified as a testifying expert on digital forensics in federal court in

UHLIG, LLC, V JOHN ADAM SHIRLEY, (CIVIL ACTION NO.. 6:08-1208-HFF)

I have also prepared expert's reports under Federal Rule 26(a)(2)(B) for the following federal civil suits filed in the United States District Court for the District of South Carolina:

Lumpkin v. Bennani, (Civil Action No. 2:03-2904-23), and
Miller v. American LaFrance Corp. (Civil Action No. 2:04-1668-23)
Microsoft v. BWC Products Inc. (Civil Action No. 2:06-CV-2023-CWH)
Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al. (Civil Action No. 2:07-CV-00673-PMD)
Mainfreight v. John Marco, et al., (Civil Action No. 9:cv00563 JFA)

I was appointed the Court's Expert in US District Court, District of South Carolina, Rock Hill Division:

The Travelers Home and Marine Ins. Co. v. Pope, C/A No.: 0:10-cv-1688-JFA

I was qualified as a computer forensics expert in North Carolina courts in:
Hollins v. Lightfoot.

In addition, I have been deposed in the following matters over the past ten years:

Thomas & Assoc. v. Christopher Humphreys (Case No. 2018-CP-10-0455)
Catherine Cope v. Wells Fargo Bank N.A., Century 21 Properties Plus, and Jim Bailey, individually; (Case No.: 2018-CP-18-00112)
Rick Gray v. Church Mutual (2017)
Calandra v. Calandra (2004-DR-10-2675)
McLernon v. McLernon (2003-DR-10-3090)
*White v. Cassidy (*2004-DR-08-256)
Khoury v. Noce (2006-CP-10-001830)
Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al. (Civil Action No. 2:07-CV-00673-PMD)
Mainfreight v. John Marco, et al., (Civil Action No. 9:cv00563 JFA)
Beard v. Dunn & Dixon-Hughes et al, (Case No. 2010-CP-08-0776)
UHLIG, LLC, V JOHN ADAM SHIRLEY, (CIVIL ACTION NO.6:08-1208-HFF)
ALTMAN, ET AL. V. FIRST CITIZENS BANK AND TRUST COMPANY (2012-CP-34-0124)

(Revised: Sept 11, 2019)