a program of zero abuse PROJECT

All the Pieces Matter

Evaluating Digital Forensic Expert Witnesses

By Christa Miller, Brandon Epstein, Joseph D. Remy, & Robert J. Peters[1]

As court cases increasingly involve the use of digital evidence, the demand for experts who can evaluate how that evidence was collected and analyzed—and then explain that process to the court— has also grown. The process by which digital evidence is identified, preserved, and analyzed is called digital forensics.

Digital forensics is a highly technical and wide-ranging field that can provide invaluable information in the pursuit of justice. But digital forensics doesn't just intersect with almost all criminal and many civil investigations: it also is poised to grow a $7 billion private-sector industry over the next five years as companies tackle security concerns.[2] This widespread demand has spawned a small army of digital

[1] This piece was originally published at www.medium.com/forensic-horizons. **Christa Miller** is Content Manager at Forensic Focus and a content writer for Zero Abuse Project. She is an expert on digital forensic issues and writes about related legal and social considerations. **Brandon Epstein** is a Digital Forensic Examiner specializing in video forensics. He has performed hundreds of digital forensic examinations involving thousands of hours of digital video and has been qualified as an expert witness over a dozen times in the past two years. He is a Certified Forensic Video Examiner (CFVE), Certified Forensic Video Analyst (CFVA), and is finishing a Master of Science degree in Recording Arts — Emphasis Media Forensics. He is active with many professional organizations, including the Scientific Working Group on Digital Evidence, the IAI Forensic Video Certification Board, the IACP Cybercrime and Digital Evidence committee, and ASTM Committee E30 on Forensic Science. He regularly provides digital forensic instruction to local, state, and federal law enforcement officers as well as attorneys nationwide. **Joseph D. Remy** currently serves as an Assistant Prosecutor in the state of New Jersey as well as on the National White Collar Crime Center's Judicial & Prosecutorial Advisory Board. Previously, he served as a Deputy Attorney General within the Financial and Computer Crimes Bureau of the New Jersey Division of Criminal Justice, as an Assistant District Attorney in the New York County Manhattan District Attorney's Office, and as a criminal defense attorney. Mr. Remy has received awards from the U.S. Department of Homeland Security and New Jersey Transit Police for his work. He frequently lectures at international and national conferences and is a Certified Cyber Crime Examiner and Certified Blockchain Expert. **Robert Peters** is Senior Attorney at Zero Abuse Project, where he develops and delivers state-of-the-art training and technical assistance for child abuse prosecutors and allied professionals. He is the creator and lead instructor of the STARK (Stopping Technology-Facilitated Abuse of Rural Kids) Prosecutor Symposium. Previously, he served as Senior Cyber and Economic Crime Attorney and General Counsel with the National White Collar Crime Center and as assistant prosecutor in multiple jurisdictions, where he specialized in the prosecution of child sexual exploitation. Mr. Peters is founder of SHIELD Task Force, a 501(c)(3) abuse prevention nonprofit.

[2] ReportLinker. "The Digital Forensics Market Was Valued at USD 4170.0 Million in 2019 and It Is Expected to Reach USD 7410.9 Million by 2025, Registering a CAGR of 10.03%, during the Forecast Period of 2020–2025." GlobeNewswire News Room, May 13, 2020. http://www.globenewswire.com/news-release/2020/05/13/2033087/0/en/The-digital-forensics-market-was-valued-at-USD-4170-0-million-in-2019-and-it-is-expected-to-reach-USD-7410-9-million-by-2025-registering-a-CAGR-of-10-03-during-the-forecast-period-.html.

forensic experts with narrow specialties. Presented with so many choices in such a technical field, how can prosecutors reasonably select the right expert for their case? This article provides attorneys with a baseline understanding to help them better assess potential digital forensic experts.[3]

What is Digital Forensics?

Digital forensics is defined as the science of identifying, collecting, preserving, documenting, examining, and analyzing evidence from computer systems, the results of which may be relied upon in court.[4] It involves the use of a computer to both obtain data from a digital device as well as analyze that data. Digital forensic examiners may also use a host of other tools to extract and examine information, from manually looking at the binary code of a file to using software that automates many examination processes. The hallmark of these examinations is that they are repeatable; the work completed by examiner A can be replicated by examiner B with the same results. This repeatability is based upon the use of quality (and tested) tools, industry standards and best practices, and effective documentation. The very purpose of digital forensics is to meet any Daubert/Frye admissibility standards and allow for introduction in legal proceedings.

What It's Not

Digital forensics has been recognized as a forensic science by numerous professional associations, government agencies, and the courts. It is not an IT function: although both professions require understanding how computers work, digital forensic techniques used to examine and evaluate evidence are wholly separate. While many computer forensic examiners may have previously worked in an IT field, IT training and experience alone does not prepare an examiner to work with evidence that could affect someone's liberty or finances in legal proceedings. For example, an IT background may indicate an understanding of how computer databases work but not necessarily where to look for timestamps in deleted data or how to recover them. Anyone who touts themselves as an IT expert, and thereby a digital forensics expert, should be evaluated cautiously as they most likely do not understand the distinction and thus lack the basic skills to complete a forensic exam.

---

[3] Zero Abuse Project does not endorse or recommend any specific expert, training class, or certification.

[4] ASTM E1732–19, Standard Terminology Relating to Forensic Science, ASTM International, West Conshohocken, PA, 2019, www.astm.org.

Digital Forensic Specialization

While the term "digital forensics" applies to examining any device that could be used as a computer system, there are distinct sub-disciplines within the field. Many experts may specialize in more than one discipline, but being an expert in one area does not make them an expert in all. Moreover, given the complexity and ever-evolving nature of technology, it is unreasonable to expect a single examiner to master all specialties. Below is a list of common disciplines within digital forensics:

- **Computer Forensics** — The analysis of data found within a computer system. Many experts specialize in specific operating systems (e.g., Windows, Mac, Linux). Computer forensics is common in both corporate and criminal investigations, but their differing burdens of proof may indicate differing goals, parameters, and, sometimes, skill sets; corporate examiners are often not required to go as deep as criminal investigators.
- **Mobile Device Forensics** — The analysis of data connected to a mobile device. Although phones now possess the processing power and storage capacity of small computers, how their data is stored and obtained is very different and requires specialized skills. Furthermore, while some experts specialize in obtaining data from mobile devices, others specialize in analyzing that acquired data.
- **Video Forensics** — The analysis of digital video. Due to the complexities of how digital video is recorded and stored, specialized knowledge is required to effectively process, enhance, and examine digital video. This fact may not be immediately apparent: many computer forensic experts (and even attorneys) attempt to perform these examinations on their own, meeting with poor results.
- **Audio Forensics** — The analysis of sound recordings. While many video forensic examiners perform audio forensics, it is a different examination with its own tools and best practices. Similarly, just as an IT professional would require specific forensic training to qualify as a computer forensics expert, an audio engineer would require specific training to qualify as an audio forensic expert.
- **Image Forensics** — The examination of imagery to draw conclusions. Examples include comparing an image to a real-world object, measuring the height of a person in an image, or determining whether an image was manipulated or changed.
- **Network Forensics** — The analysis of network traffic to answer questions about activity, including intrusion detection and response.
- **Malware Analysis** — The evaluation of computer viruses and illicit programs to determine security risk, mitigation, or origin.

- **Vehicle Forensics** — The extraction and analysis of data from embedded vehicle infotainment systems (e.g., Sync, Onstar, other GPS systems).
- **IoT device Forensics** — The analysis of data from non-traditional computer sources, such as drones and home automation systems, often by directly accessing the computer chip on the device. IoT and mobile device forensics may overlap, with some examiners specializing in directly accessing the chip on cellular devices.

Do I Need an Expert?

Attorneys may not immediately recognize when they need a digital forensic expert. Unfortunately, the need for an expert is often not apparent until inside a courtroom. Perhaps the greatest example of this oversight is the nationally televised mishandling of computer evidence during the trial of Casey Anthony in 2011. Law enforcement had missed key evidence on the computer's web browser history—evidence, it was later revealed, that the defense's forensic experts had discovered prior to trial.[5] In a different example of poor expert selection, the state retained two audio forensic experts in the prosecution of George Zimmerman in 2013 to provide opinions about 9–1–1 recordings critical to their case. A Frye hearing was conducted on the eve of trial and resulted in the two experts being barred from testimony, with the judge noting, "there is no evidence to establish that their scientific techniques have been tested and found reliable"[6] and that their testimony "would confuse issues, mislead the jury and, therefore, should be excluded from trial."[7]

Clearly, it pays to be prepared. While the vast majority of criminal cases end in plea bargains[8] and not in national headlines, digital evidence should be treated as if the case will proceed to trial. Aside from the unique nature of digital evidence acquisition and sheer volume, binary data must be analyzed and processed in a way that is easy for investigators and attorneys alike to read and search the results. Even then, be mindful that data could be interpreted with different, and possibly incorrect, meaning by the untrained eye.

---

[5] T. Pipione, "Cops, prosecutors botched Casey Anthony evidence," 28 November 2012. [Online]. Available: https://www.clickorlando.com/news/2012/11/28/cops-prosecutors-botched-casey-anthony-evidence/.

[6] S. Tienabeso, "George Zimmerman Judge Denies Use of State Audio Experts' Testimony," 22 June 2013. [Online]. Available: https://abcnews.go.com/US/george-zimmerman-judge-denies-state-audio-experts-testimony/story?id=19463576.

[7] R. Stutzman and J. Weiner, "Judge bars audio experts from George Zimmerman trial who say screams were not his," 22 June 2013. [Online]. Available: https://www.orlandosentinel.com/news/trayvon-martin-george-zimmerman/os-george-zimmerman-trial-experts-ruling-20130622-story.html.

[8] G. Del Valle, "Most criminal cases end in plea bargains, not trials," 7 August 2017. [Online]. Available: https://theoutline.com/post/2066/most-criminal-cases-end-in-plea-bargains-not-trials?zd=1&zi=i67joto4.

How Do I Find an Expert?

Before you can evaluate an expert, first you have to find one. Unfortunately, there is no single list of vetted digital forensic experts or Consumer Reports ranking. The search process is similar to finding any specialist, be it lawyer, mechanic, or accountant: word of mouth, referral services, and internet searches all play a role.

Obtaining a referral from a trusted colleague or even by general reputation is vastly preferable to running a generic internet search. To be expected, a simple Google search for "digital forensic expert" returns a daunting list of results and starting here will require a considerable amount of work to ensure you've found the best person for the job.

An alternative to internet searches, lists of certified examiners are published online by many certifying bodies. These discipline-specific lists can help winnow in on the best possible expert. (Note: The following list is not exhaustive, nor does inclusion indicate an endorsement.)

- **Computer Forensics**
  - International Association of Computer Investigative Specialists (IACIS) — Certified Forensic Computer Examiner
  - Global Information Security Certification (GIAC) — Certified Forensic Analyst/Examiner
  - International Society of Forensic Computer Examiners — Certified Computer Examiner
- **Mobile Device Forensics**
  - GIAC — Certified Advanced Smartphone Forensics
  - Cellebrite Digital Intelligence — Certified Mobile Examiner
- **Video Forensics**
  - International Association for Identification (IAI) — Certified Forensic Video Examiner
  - Law Enforcement and Emergency Services Video Association (LEVA) — Certified Forensic Video Analyst

Regardless of how you compile your short list, two quick indicators of a candidate's expertise and integrity include their website and their business address. In most circumstances, an expert's website is their attempt to put their best foot forward and impress potential clients. The site should be evaluated for content as opposed to entertainment value: a particularly flashy website lacking basic information like qualifications or specific services may be a red flag. On the other hand, a website that touts a single examiner as an expert in every area of digital forensics should be evaluated with an equally critical eye.

Also pay special attention to any addresses listed on the website. Many experts work out of their home and, therefore, may use a post office box or similar service for their business address—an understandable practice. However, some experts obtain mailing addresses in desirable cities like New York, Chicago, or Los Angeles—regardless of where they actually work—to give the false impression that they have multiple, high-priced locations.

How Do I Evaluate an Expert?

Evaluating Their CV

An easy way to obtain a general overview of a digital forensic expert's abilities is by reviewing their curriculum vitae. Intended to document education, qualifications, and experience, a CV is also a marketing tool for showcasing skills and demonstrating value. While a CV may contain a wealth of impressive information about a potential expert, it should be evaluated with a critical eye, ensuring that the information presented is relevant and helpful to the particular case at hand.

Education

Formal Education. Education is a major component in any expert's CV, including digital forensic experts'. When evaluating an expert's education, it is helpful to remember that digital forensics is a forensic science, not a computer science or IT function. That being said, digital forensics is a relatively new field, and degree programs are limited. An expert's knowledge base may have been acquired outside a formal degree program. Similarly, experts with law enforcement backgrounds, such as a degree in criminal justice or completion of a police academy, are not necessarily prepared for complex digital forensic examinations.

Continuing Education/Training. Aside from formal education, the vast majority of knowledge gained by a digital forensic examiner comes from training courses outside a college or university environment. Independent trainings can also be some of the hardest entries on a CV to evaluate for legitimacy and relevance.

Trainings can be broken down into two general categories: "vendor neutral" courses that are not tied to a specific commercial tool but concentrate on overall theory and procedure; and courses that are designed to show how to operate and understand a specific tool as part of an examination. Both types of courses are important in gaining digital forensics knowledge. For an analogous example, vendor neutral training would show how plumbing in a house should be connected for effective drainage but would not show you how to join individual pipes. The wrench vendor, on the other hand, would

demonstrate how to use their tool to effectively connect pipes but would not tell you how to configure the plumbing system.

When evaluating training, it is also important to discern between actual training classes and informational sessions—often thinly veiled sales pitches. Increasingly, vendors are offering one-hour (often free) webinars on a specific tool or function. It is easy for an unscrupulous examiner to list every webinar as a separate training and quickly fill pages of a CV with impressive sounding but ultimately meaningless course titles.

Two elements that could help evaluate the depth of a training are the number of contact hours required as well as the delivery method (online or in-person). There are many quality online trainings but there are an equal number of unaccredited and unreliable courses. It is easy to have a 90-minute webinar appear as a 40-hour in-depth course without context. If course hours are not listed on a CV, some follow-up inquiries may be necessary. While a long list of short online trainings may merely indicate budgetary or other resource challenges, attempting to pass those courses off as in-depth study may signal a larger concern with the expert.

Certification. Certification in digital forensics can be a strong indicator of proficiency, but like training courses, not all certifications are equal. A certification could be as meaningful as in-depth written and practical proficiency testing or little more than a piece of paper received for course attendance or payment of a fee. Differentiating between the two can be difficult, especially because many less reputable certifications will mimic high-quality programs. For example, a certification from the American College of Forensic Examiners Institute (ACFEI) sounds impressive, but a quick internet search reveals it to be mired in controversy and accusations of fraud.

Many reputable certification programs make an effort at transparency. They may name certificants and provide information about the evaluation process. They may also hold requirements regarding minimum hours for training or other experience, as well as written and practical application tests. As part of a larger initiative to improve forensic science across the country, there has been a recent push to independently review and accredit certification programs. While those accreditation programs themselves may warrant research to determine their legitimacy, this validation could signal a quality certification program. Certifications are also offered by software vendors who develop the tools used in the field. While it's sensible for examiners to be certified in the tools they use, their qualifications should be well balanced, and include independent certifications or other indications of knowledge relating to overall workflow and theory.

It is noteworthy that while organizations certify examiners, courts do not. A court may qualify an expert in a certain discipline, but that qualification is specific to the matter at hand. An expert who claims to be "court qualified" could be playing semantics, but experts who purport to be "court certified" may very well have crossed a line.

Despite the effort required, evaluating the quality of certification programs is time well spent—either to unveil unqualified and potentially unscrupulous candidates or to discover true experts. The payoff is presenting the most accurate evidence in court, with appropriate weight given to your expert's testimony. Foregoing due diligence here risks disastrous consequences—as when opposing counsel points out that your expert was awarded the same certification as a journalist's cat.[9]

Experience

A strong indicator of a forensic examiner's ability to provide compelling testimony is their record of providing such testimony. Noteworthy elements include the number of times an expert has been qualified, in which specific disciplines, and the location and type of court. While it may be easy to qualify an expert in computer forensics for the 26th time in a particular state, the same may not hold true if that expert is hired to perform audio analysis in a federal court across the country. Additional attention should also be paid to the expert's experience in depositions (in civil cases) as well as any Daubert/Frye hearing in which they have participated.

Presentations

For experts without much courtroom experience, one good indicator of their potential is having conducted formal instruction or other presentations on digital forensic topics. Much of the testimony of a digital forensic expert involves educating the trier of fact on complex technological issues. As such, when looking at training presentations, pay special attention to the audience and venue. A conference presentation to other professionals on a novel technique or method has an entirely different communication skill set than an internet safety talk to a local Boy Scout troop. Ideally, the expert will have a well-rounded mix of audiences; however, less technical presentations may not appear on a CV. It may be worth following up with the expert to determine if they have experience relating technical terms to a lay audience.

---

[9] See e.g., ProPublica, "No Forensic Background? No Problem," 17 April 2012. [Online]. Available: https://www.propublica.org/article/no-forensic-background-no-problem.

Publications

Contributing to the digital forensic community by publishing information can distinguish a top-tier professional from an average expert. Like with other aspects of an expert's CV, any publications should be evaluated with a critical eye. A peer-reviewed scientific journal article—a thoroughly vetted publication with a professional readership and an outsized impact—carries far more weight than an expert's blog post on their own website. Given the rapidly changing nature of digital forensics, however, some peer-reviewed digital forensics and incident response (DFIR) blogs could be respectable publishing avenues. Note that abstracts for conference presentations may appear as published work; at face value, the titles for these potentially half-page submissions could look identical to extensively researched multi-page journal articles. To gain a better sense of the work in question, run an internet search for the published work or follow up with questions to the expert regarding the type of submission and review process. The presence of a Digital Object Identifier (DOI) number on the search results may help indicate which works are notable published resources. Like many other areas of the CV, there is a line between an expert trying to accurately describe their work in the best light possible and embellishing their accomplishments.

It is common for an expert to not have any published works, and their absence alone should not set off alarm bells. Research and publishing are not job functions of many digital forensic experts, in either the government or private sector. Many are simply too busy working actual cases and are not compensated for publishing. On the other hand, a strict academic with dozens of published works may lack the real-world case and testimony experience necessary to be effective in the courtroom.

Professional Memberships

Because digital forensics involves fast-changing technology, experts must stay abreast of advancements in the field. Membership in relevant professional organizations can be a good way to stay connected within the digital forensic community. While some organizations restrict membership to a particular profession (e.g., law enforcement), there is no shortage of groups whose purpose is to share information among practitioners. When evaluating professional memberships, the expert's role within the membership organization is an important factor. Did the expert merely pay dues for seven years, or did they attend meetings, participate in committees, or otherwise contribute to an exchange of ideas as reflected on their CV? Follow-up questions could help determine their level of engagement.

Public vs Private: Does It Matter?

Digital forensic experts are found in both the public and private sectors. While there are patterns of work experience particular to each sphere, both paths can provide relevant experience, and an expert's background should be evaluated on the totality of their qualifications as they relate to the case at hand.

- **Public-sector** digital forensic experts work with law enforcement across government agencies on criminal (and sometimes civil) investigations. They are likely to have attended a large number of trainings and worked on many actual cases. They may not have a background or education in any kind of forensics or computer science prior to their assignment as a digital forensic examiner. Their experience is also most likely concentrated on the prosecution of criminal acts, with little or no experience working as a defense expert, at depositions, or in the corporate or civil arena. Many digital forensic experts who begin their career in the public sector later work in the private sector.

- **Private-sector** experts may have a background in computer science or other related education but less training specific to digital forensics than their public-sector counterparts—often due to issues of cost or access. Private experts may have had more experience with different areas of the legal system; they may also have had less actual case or testimony experience.

While a CV details pertinent aspects of a digital forensic expert's work history, training, and qualifications, evaluating actual work products and outcomes will provide a clearer picture of their talents in the field.

Testimony

An internet search of an expert's name can provide helpful information regarding their work history. Specifically, searching for news articles covering an expert's testimony may give insight into their effectiveness on the witness stand. Search results may even contain video clips of testimony in a trial or deposition, letting you observe their ability firsthand.

Sample Report

Experts should also be able to provide a sample report to any potential client. Even if a complete report is not available, a redacted version to evaluate the expert's work product should be.

Methodology. Aside from overall spelling, grammar, and readability, the report and any accompanying notes should have enough detail so that another examiner could complete the same work and evaluate the results. The report should also include references to any specific terminology, method, or technique employed. It is prudent that any report which generates an expert opinion be peer-reviewed for accuracy and validity.

Proficiency with Forensic Tools. A sample report could also provide insight into the tools an expert uses to complete their examination. Digital forensic software can be expensive, particularly for sole-practitioner experts but for small law enforcement agencies as well. Many examiners employ the use of freeware tools in their work, and that alone does not signify a lack of quality. What's important is that the expert validate the tool or verify that it works correctly before using it. The expert should be able to explain how they validated and verified the tool during follow-up questioning or through written documentation of the testing process. These procedures may also be communicated through a written policy or procedure manual in the expert's workplace.

Red Flags

Terminology. For many years, the phrase "reasonable degree of scientific certainty" was a staple of expert reports. It is also a good indicator of an expert who stays abreast of the latest trends in forensic science: as part of ongoing attempts to improve forensic science in the United States, in 2015 the now-defunct National Commission on Forensic Science cautioned that the phrase was ambiguous and potentially misleading. The Department of Justice heeded this warning and in 2018 advised all of its

experts to cease using the term;[10] many other experts followed suit for the same reasons. Use of this language in a recent expert report may give reason for further evaluation.

Bias. Bias is a concern within all forensic science, and a skilled forensic expert should be able to articulate how they minimize bias in their work. Efforts can include limiting unnecessary knowledge of the case, following the scientific method, or other articulable means.

Compensation. As part of the concern to reduce bias, experts should also refrain from entering contingency fee agreements, even where allowable. Regardless of who hires the expert, their work should remain impartial; tying the compensation of the expert to the potential outcome of the case may influence that impartiality. Any expert who will enter into such an agreement should be evaluated cautiously. An expert who will contract directly with a private individual (not an attorney, firm, or investigation service) should also raise red flags.

Evaluating an Opposing Expert

It may require some time and effort to identify your own qualified expert for the case at hand, and equal time and effort to evaluate any opposition. However, once you have retained a digital forensic expert, they should be able to assist in evaluating any experts hired by opposing counsel. It is not uncommon for digital forensic experts to maintain dossiers on others in the field, particularly in smaller disciplines. That information could be worth its weight in gold when attempting to impeach an expert's testimony. For this reason alone, it may be worthwhile to hire an expert whenever the opposition has retained one.

[10] National Commission on Forensic Science. Available: https://www.justice.gov/archives/ncfs/page/file/641331/download.

Conclusion

As a science, digital forensics is owed the rigor of other sciences. Just as forensic examiners rely on tested theories and tools to achieve repeatable, reproducible results, attorneys rely on expert witnesses to testify effectively about those methods and results on the stand. Because the science can be complicated to communicate, expert qualifications are difficult to ascertain—especially in an ever-shifting landscape. Finding, evaluating, and verifying experts is well worth the time and effort for the impact it has on science, liberty, and justice.

 This project was supported by Award No. 2019-CI-FX-K006 awarded by the Office of Juvenile Justice and Delinquency, Office of Justice Programs, Department of Justice.