Cyber Forensics Training for Judges

Ryan Whytlaw, Christie Nelson, and Dennis Egan
CCICADA Center, Rutgers University

June 29, 2020

For Further Information Contact: Dennis Egan (deegan@dimacs.rutgers.edu)

Cyber Forensics Training for Judges

Ryan Whytlaw, Christie Nelson, and Dennis Egan
CCICADA Center, Rutgers University

June 29, 2020

1. Abstract

The Command Control and Interoperability Center for Advance Data Analysis (CCICADA) at Rutgers University was funded by the U.S. Department of Homeland Security through the George Mason University Criminal Investigations and Network Analysis Center (CINA) to conduct a cyber forensics training needs assessment project. The original project focused on the cyber forensics training needs for DHS and State and Local law enforcement. While conducting interviews with law enforcement officials (e.g. county prosecutors, district attorneys, and cyber forensics experts), it became apparent that training judges and attorneys in cyber forensics was a critical need. This paper outlines the growing strains on the court system that rapidly advancing information and communications technology is placing upon the legal community and the expanding knowledge base practitioners need to effectively conduct business within the court system. The growth and advancement of such technology is outpacing the ability for the legal system to maintain applicable standards in cyber forensics and therefore requires the problem to be addressed through effective and adaptable training, legislation, and information management.

2. The Need

With the challenges facing law enforcement and the rapid pace of technology change, even more focus may be spent by judges and attorneys alike on applying standards of admissibility of digital forensics expert testimony, reporting and evidence while keeping track of changing legislation across the country. Questions include: what constitutes a qualified examiner and subsequently a reliable and accurate digital forensics report; what technology exists and how do judges and attorneys maintain awareness of evolving advancements; how do changes in domestic laws and the potential influence of international laws impact cases; and how do judges and attorneys handle the increased volume of electronically stored information (ESI). These and related issues are increasingly raised within the court system today.

Cyber forensics faces a number of challenges including:

- Lack of industry training standards (though some organizations have begun to establish standards and certifications, not all have been validated/vetted by DHS);
- Rapidly evolving technologies and advancement in encryption;
- National/International legislation restricting information seizure; and
- Data volume (and the cost associated in storing and searching such data). (Sadiku, Tembley, & Musa, 2017)

Thumma and Wildeman (2017) found that "significant challenges to providing effective judicial forensic science education exist everywhere." In conducting a needs assessment across the state of Arizona, a Forensics Workgroup found that general jurisdiction, limited jurisdiction and appellate judges all identified a 'strong interest' in digital forensics. "For all three categories of judicial officers, the most frequently selected response to" the interest in computer/electronic topics "was information about data recovery from cell phones and handheld devices" (Thumma & Wildeman, 2017).

This paper explores the various requirements cyber forensics, and subsequently electronically stored information (ESI), places upon the judicial systems of the United States. We will further outline that these requirements have created a need for both judges and attorneys to obtain additional knowledge relating to cyber forensics and evidence, along with other gaps in training that could be recommended. We will continue to detail throughout this white paper the need for additional training be given to judges in the areas of digital forensics, eDiscovery, electronically stored information (ESI), and rapidly changing legislation around these topics. We will further detail our recommendations after illustrating our findings from original research and interviews of SMEs.

3. Some Useful Definitions and Distinctions

This white paper is focused on training judges and attorneys on cyber forensics. The term cyber forensics encompasses both *computer* forensics focused on investigations of computers and *digital* forensics focused on investigations of many kinds of digital devices including cellphones, digital cameras, and the wide array of Internet of Things (IoT) devices.

E-discovery is a process complementary to cyber forensics. Since both cyber forensics and e-discovery involve electronically stored information (ESI), and both are used in criminal and civil investigations, it is important to distinguish between them[1]. E-discovery is a multi-step process in which admissible evidence is identified, collected, filtered to remove duplicates, useless, and privileged information, and then produced for use by investigators and attorneys. The information may be documents, emails, spreadsheets, and data available on disk drives, other media, or in cloud storage. In many cases, e-discovery involves huge volumes of information and the process is carried out by a third-party firm that specializes in the process.

Cyber forensics is a discipline used to obtain evidence that must be extracted by specially trained experts who work to obtain information that may be hidden, encrypted, or deleted but not destroyed, etc. The evidence is typically on smartphones, personal computers, and thumb drives. The information typically includes emails, messages, location tracking data, browsing histories, contact lists, etc. Cyber

[1] A more thorough discussion of the differences between E-discovery and cyber forensics can be found at: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/computer-forensics-investigations/e-discovery/#gref .

forensics experts can apply a range of extraction techniques that vary in terms of required technical sophistication and specialized software and hardware tools.

4. Background and History

As the Information Age made resounding advances in computational processes and capabilities, the cultural reliance upon information and communications technology (ICT) grew from industrial business users to individual worldwide consumers. The usage of ICT broadened, resulting in computers supporting something as large as electrical grids and national economic systems to something as small as counting steps of an individual throughout the day. ICT has inherently changed society itself (Henseler & van Loenhout, 2018). Coupled with the advancement of the internet and its capability to transfer and calculate significant quantities of information, law enforcement, judicial systems and even individuals around the world have had to react to the ever-growing legal implications of utilizing devices for most aspects of one's personal and business activities.

The continued growth and advancements in digital technology has put increased demand upon all parties involved in both civil and criminal law to understand various aspects of cyber forensics. Primarily used in large corporate complex settings in the past, the increased use of various devices using word-processing, e-mail, databases, messaging services, among many other types of electronically stored information has become "a routine feature in litigation. ((Hedges, Rothstein, & Wiggins, 2017). According to NIST, "digital forensics, also known as computer and network forensics, … is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data" (Kent, Chevalier, Grance, & Dang, 2006). The consumption of digital information has now squarely placed cyber forensics before the U.S. court system at all levels requiring judges and attorneys alike to make decisions based upon their understanding of cyber forensic science.

Under the Federal Rules of Evidence (FRE) Rule 702 "a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case" (One Hundred Fifteenth Congress, Committee on the Judiciary, 2017). However, states have the authority to adopt their own rules. Through the later part of the 20th century, the Frye standard was widely used by states throughout the country requiring that evidence, such as scientific testing and subsequently the results of those tests, are inadmissible if the method or process has not gained recognition from the scientific field and community. It was not until the 1993 Daubert v. Merrell Dow Pharmaceuticals Inc. decision that evidence standards began to change at the state level. "The United States Supreme Court held that the Federal Rules of Evidence, and in particular Rule 702, superseded Frye's 'general acceptance' test" (National Forensic Science Technology Center, 2013). This decision also outlined five (5) standards for

judges to apply to “any scientific procedure used to prepare or uncover evidence” to determine whether the evidence is admissible in federal court (Garrie, 2014). The standards include:

- Whether the theory or technique can be or has been tested
- Whether it has been subjected to peer review and publication
- Whether its error rate is known and acceptable
- Whether standards controlling its operation exist and are maintained
- Whether it has been accepted within the relevant scientific community

As a result, states began adopting the federal standards or a modified version thereof. According to Garrie, the Daubert standard reigns as the one recognized by most jurisdictions across the country. However, Frye remains the primary standard in some locales (McDonough & Jacqueline, 2018). The debate between the two standards continues today across the country and within the court system. Although these standards precede the field of cyber forensics, they remain the applicable standard to cyber forensic science throughout the judicial system.

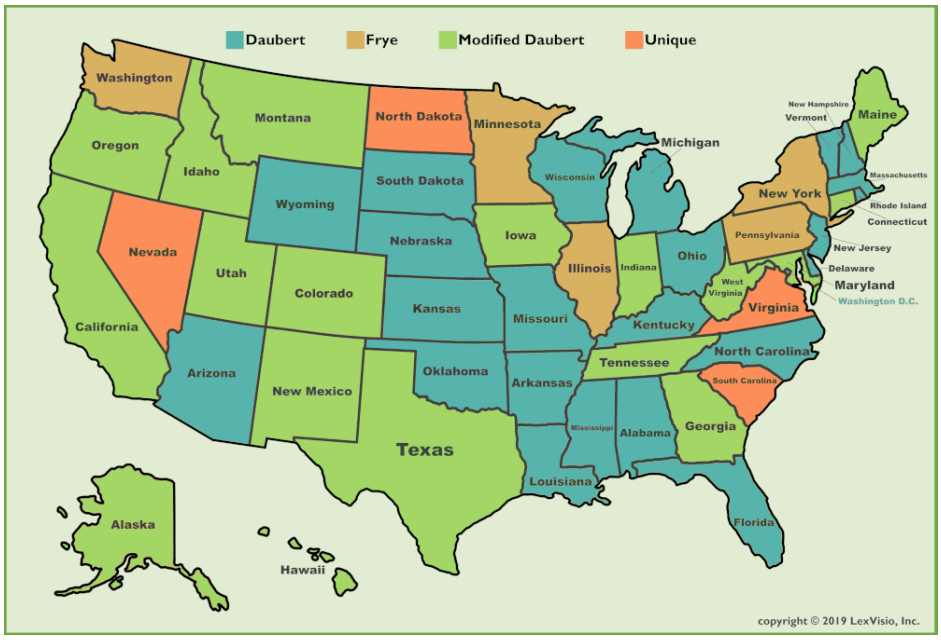

Figure 1: Daubert v Frye Standards Across the United States (Hill, 2019)

Nonetheless, some individuals hypothesize that the standard a jurisdiction follows is inconsequential (Chang & Yoon, 2005). Chang and Yoon have theorized that Daubert has simply raised the awareness of the judiciary community about unreliable scientific evidence. In 2002, Dixon and Gill found that after Daubert, judges tightened their standards for admitting expert evidence and are more likely to evaluate the reliability of expert evidence (Dixon & Gill, 2002). Regardless of the applied standards, judges and attorneys alike need to be aware of the advancements of science and the resulting impacts on all cases.

Soon after personal computers were being offered widely to the public, the FBI established the Computer Analysis & Response Team (CART) in 1984 to aid in digital investigations. Throughout the

technological advancements of the 1990's the law enforcement community established organizations to keep up with the resulting growth and the advent of the world wide web and public internet. In the late 90's the Scientific Working Group on Digital Evidence (SWGDE) formed and by the early 2000's the FBI began the construction of their Regional Computer Forensic Laboratory (RCFL) and the corresponding National Program Office (NPO). Today, digital forensics is practiced not just by law enforcement agencies, but also by many commercial industries and private businesses. Increasingly, forensics experts might be called to support the prosecution or defense or both during criminal trials. The same may apply to plaintiffs and defendants in civil trials. Judges will be expected to have the background to rule on forensics experts' qualifications, reports, and testimony.

5. Knowledge Gaps for Judges in Cyber Forensics

We have identified five topic areas in cyber forensics where judges could use specific additional education and training. The topic areas are Cyber Forensics Standards and Procedures; How Technological Advancements Affect Standards; Electronically Stored Information (ESI); Evolving Legislation; and Encryption and Passwords. From the interviews we have done, it is clear that the federal judiciary has greater education and training opportunities and resources than states can provide to their judges, and that states may differ greatly in terms of their available resources. We will return to this issue in our section on recommendations.

5.a Cyber Forensics Standards and Procedures

Judges should be able to scrutinize forensics examiner qualifications, considering certification, education and experience (Garrie, 2014) of examiners and the appropriate practical qualifications examiners need. Judges and attorneys need to understand forensics reporting and the contents that produce a reliable and accurate forensics report. Currently there are many digital forensics certifications offered by government agencies, for-profit and non-profit training organizations, software and hardware vendors, and even some colleges. Yet, there is no one central authority vetting these myriad offerings, placing the burden on the court to judge their validity as they come up in individual cases.

In 2010, Kesler concluded that "judges recognize that they need additional training in computer and Internet technology … This training would enable judges to better understand the arguments presented by lawyers, testimony offered by technical witnesses, and judicial opinions forming the basis of decisional law" (Kessler, 2010). The lack of training continues a decade later. Through interviews for this research, experts in the field have continued to identify the lack of training for judges specifically in the area of cyber forensics to be a primary training gap. The lack of knowledge has led to the need for judges to be educated by prosecutors on cyber forensics during the processes of writing and requesting warrants. Although one interviewee stated judges are not meant to be experts in everything that comes before them, cyber forensics that increasingly will come before them in all types and levels of court is something worth additional training. We were also told in an interview that judges cannot base their decisions in areas for which they have not received formal training, e.g. smart phones, even if they have

acquired personal knowledge in such areas. In general, it is essential that training is provided to allow judges to evaluate forensics evidence (Thumma & Wildeman, 2017). Further, there is a "need to focus educational efforts on both criminal and civil matters (including family law, probate, and other types of noncriminal matters)" (Thumma & Wildeman, 2017).

Efforts have been made internationally to set standards for digital forensic experts. In 2015, the Netherlands Register of Court Experts (NRGD) set standards and requirements for digital forensic experts (Henseler & van Loenhout, 2018). The standards span a number of subfields within digital forensics and recognizes the fact technology will continue to expand requiring the experts themselves to identify limitations in their qualifications (Henseler & van Loenhout, 2018). Further, it outlines the needs for coordination amongst experts as complex cases may require multiple experts as highlighted by 'Dagger', a case involving the hacking of the shipping industry for the purposes of drug trafficking at the port of Antwerp. Henselar & van Loenhout (2018) also point out similar efforts have been undertaken in the United Kingdom and the European Union while in the United States there has been "less emphasis on the certification of individual experts" and more focus has been largely on certifying tools and processes such as the efforts of NIST and the work SWDGE has done on addressing the ISO17025 standard (Henseler & van Loenhout, 2018). With less focus on developing a single judicial standard and certification for experts to meet, the approach in the United States requires judges to have an increased knowledge base on cyber forensics and its subfields. The growing industry of cyber forensics certifications coupled with the judge's responsibility as gatekeeper to the court places an ever-growing need for judges to be trained in the field.

5.b How Technological Advancements Affect Standards

Once digital forensics training standards are established, how will the standards address the frequency with which the technology advances to maintain relevance? The second major issue facing the judicial system is the fact that technology is advancing so rapidly, prior applicable judicial standards such as Frye or Daubert cannot possibly be met. Sommer points out that "the speed of change is much faster than the rate at which an artefact with evidentiary potential can be identified and analysed, written up in a peer reviewed journal article, published and then made the subject of a reliable tool – which itself would then need to be validated" (Sommer, 2018). Sommer continues highlighting the potential concerns facing the law enforcement community whereas new applications, social media or a messaging service gains significant and rapid presence in the marketplace without an approved verified scientific forensics technique. This becomes a potentially more problematic issue when experts are forced to conduct physical examinations of digital evidence using techniques such as chip-off or JTAG. Experts we have interviewed have also highlighted the potential problems associated with this, specifically spoliation. If damage occurs to the physical evidence and the other party is unable to conduct its own expert assessment, any evidence gathered would be barred from use at trial.

For example, the International Organization for Standardization (ISO) has outlined specific requirements for competence of testing and calibration laboratories under ISO Standard 17025. As Sommer points out, how would this particular standard hold up when the technology itself is updated frequently? Consider the frequency in which operating systems of personal computers or cell phones occurs and the

time it will take just a single update to pass through rigorous testing, validation and acceptance in the scientific community. “New advances in computer forensics technology will continually raise reliability issues, particularly as new techniques are deployed in the field without extensive review” (Goodison, Davis, & Jackson, 2014). It will be months or years before some scientific processes will meet the standards outlined in Daubert if strictly applied in court. Not only will this cause further delays in court proceedings or the admissibility of critical evidence be rejected but as the Scientific Working Group on Digital Evidence (SWGDE) has pointed out, digital and evidence forensic practitioners “struggle to establish their confidence on a scientific basis” (Scientific Working Group on Digital Evidence, 2018). According to Sommer, “there is no single “one size fits all” route to assuring quality in digital forensics evidence” (Sommer, 2018).

As the SWGDE outlines in their paper ‘Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis’, “some forensic disciplines use an error rate to describe the chance of false positives, false negatives, or otherwise inaccurate results when determining whether two samples actually come from the same source. But in digital and multimedia evidence forensics, there are fundamental differences in the nature of many processes that can make trying to use statistical error rates inappropriate or misleading” (Scientific Working Group on Digital Evidence, 2018). Therefore, meeting standards such as the ISO 17025 or the criteria under Daubert becomes difficult. SWGDE recommends the development of a “more formalized approach to handling potential sources of error in digital and multimedia evidence forensic processes.” Sommer echoes a similar approach recommending giving discretion to judges to apply best practices and guidance on a case by case basis. In the end, “no amount of testing can prove that [multimedia or digital forensics] tool is functioning correctly in all instances of its use. Even if all tests produce the expected results, a new test scenario could reveal unexpected results” (Scientific Working Group on Digital Evidence, 2018).

5.c Electronically Stored Information (ESI)

In addition to the forensic aspect to the training gaps that plague some court systems, judges have already been relied upon as experts of sorts in ESI and related technology as part of the discovery process. Judges have found “discovery involving ESI may require more intensive judicial involvement than required by conventional discovery” (Hedges, Rothstein, & Wiggins, 2017). Even as technology assisted review (TAR) tools are becoming increasingly useful in expediting the discovery process, other discovery methods are still eligible for use. With both processes legally available to prosecutors and defendants across the country, judges are increasingly expected to be able to understand the technology behind both.

Under the keyword search method, judges generally rely upon the parties to agree upon the searchable terms. However, “there are a number of cases where courts are presented with ESI scope disputes over keywords. In these cases, courts generally will either order certain keyword searches to be performed or that search terms be modified by applying proportionality principles” (Broughel, Worthington, Barnett, & Ehmke, 2018). In some cases, to expedite the process, the judges have become involved in identifying hundreds of potential search terms (O'Connor, 2017). This process requires some understanding of data

mining, a topic not typically well understood by judges. It has been recommended that judges shouldn't just dictate search terms without seeing what is returned. This highlights an educational gap in an expertise that judges are expected to have about digital evidence. It is recommended that judges suggest search terms, test them, then think if there may be variations, and reiterate. (O'Connor, 2017). As for the use of TAR, "When disclosure occurs, and parties cannot agree about the TAR process to be used, a judge may need to determine whether the producing party's proposal is reasonable. This is a risk for a producing party, as judges vary in their familiarity and views on different approaches to TAR." (Bolch Judicial Institute, Duke Law, 2019) TAR itself is a machine learning process consisting "of several steps, including collection and analysis of documents, training the computer using software, quality control and testing, and validation. (Bolch Judicial Institute, Duke Law, 2019) It also represents another area where the legal community needs to increase its understanding.

In 2012, a case between Apple Inc. and Samsung resulted in the collection and processing of 11,108,653 documents by Samsung over a 20-month period. This amounted to 3.6 terabytes of data at a cost of over $13 million. (logikcull, 2020) The 2016 Joint Technology Committee Resource Bulletin: Managing Digital Evidence in Courts, warned that "[c]ourt management systems are not currently designed to manage large quantities of digital evidence, which means that courts and industry must find creative ways to deal immediately with the dramatically increasing volume of digital evidence, while planning for and developing new capabilities." (Arizona Task Force on Court Management of Digital Evidence, 2018).

The state of Arizona established a Task Force that went on to recommend a number of actions to address the issue including requiring the submission of digital evidence in standardized formats (with exceptions), the establishment of best practices for digital evidence management solutions while considering costs, and the establishment of technical requirements at various levels of the court system to address ESI as it relates to storage solutions (Arizona Task Force on Court Management of Digital Evidence, 2018).

However, some orders of the courts have similar ramifications external to the court as well. An order to preserve evidence can place undue burdens to the party required to preserve ESI, while not ordering the preservation may hinder the other party from prosecuting/defending actions (New York State Unified Court System's E-Discovery Working Group, 2015). We have even found that judges can be dictating key word searches to be used in email recoveries, where judges don't know that one set of keywords may be more useful, or that two sets of keywords are similar but one search term can be much cheaper in terms of data storage and recovery. Who the burden of this falls on to determine such search terms is often unclear. The New York Bench Book regarding ESI states that "with respect to preservation orders, judges are cautioned against entering a preservation order without more fully understanding the types of ESI that must be preserved, the format of their preservation, the costs to be imposed by such preservation and the extent to which such preservation will interfere with the ordinary course of the responding party's business operations" (New York State Unified Court System's E-Discovery Working Group, 2015). In 2002, the Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG) recommended that "when producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has

already done or would do for its own case preparation or discovery production" (Joint Working Group on Electronic Technology in the Criminal Justice System, 2012). This reflects that "e-Discovery not just for civil litigation — and it hasn't been for some time. (Sullivan, 2018)" Subsequently, ESI is also increasing in its availability and use in both civil and criminal matters.

5.d Evolving Legislation

In trying to address the evolving changes in forensic science, there have been many changes to the law (Thumma & Wildeman, 2017). Changes in laws may also be prompted due to constraints of the court system itself. In 2015, the Federal Rules to Civil Procedure (FRCP) changed drastically. The changes refined and outlined the "considerations of whether information should have been preserved, and specifying measures a court may employ if information that should have been preserved is lost and cannot be restored or replaced" (Henry & Palacios, 2015). As digital evidence and digital forensics presence within cases surge considerably, judges' and attorneys' awareness of the volume constraints that electronically stored information (ESI) create also grows. On December 1, 2017, sections 13 & 14 to Federal Rule of Evidence 902 became effective, streamlining the process of authenticating electronically stored information (ESI) and admitting it into evidence (O'Neill, 2018). Rule 902(13) states "a record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11)" (O'Neill, 2018). While improving the process for admissibility in the court system, the new rule also furthers the interdependence of the core issues digital evidence raises within this paper. The authenticating authority still must meet certification standards as determined as sufficient by the presiding judge which can become difficult. As O'Neill points out, "the rule's commentary recognizes that changes in technology may give rise to other methodologies" (O'Neill, 2018). However, the rule does provide flexibility to "to allow certifications through other reliable means of identification that become available with future technology" while also limiting costs associated with obtaining and ensuring admissibility of ESI evidence (O'Neill, 2018).

However, it is not just U.S law that is making frequent changes. Europe is also trying to address the frequent and increasing advancements in digital and cyber forensics. This not only impacts Europe but the U.S. as well in that it is possible that data entered into a system may be done in the U.S. while the data itself may be stored abroad, or vice versa. These impacts have been brought to the highest court in the country. Cases are being heard that may result in a decision being rendered in which new rules coming out of Europe impact the U.S. courts. The court system as a whole may then need to be aware of potential impacts international law on digital evidence may have on U.S. rulings (Austin & O'Connor, 2018). This raises the possibility that judges may need additional education and awareness in aspects of international law.

5.e Encryption and Passwords

A number of recent cases and court decisions have focused on law enforcement agencies' attempts to break encryption codes or acquire passwords protecting potential evidence. These are recent cases, so judges should be aware of evolving case law and the possibility of legislation in the near future.

One example concerned the San Bernardino Mass Shooting in 2015. The FBI wanted Apple to unlock the work iPhone of the alleged attacker (Syed Rizwan Farook). Farook and his accomplice had destroyed their personal iPhones, but the FBI recovered Farook's intact work iPhone that was owned by his employer. New encryption technology required the FBI to have the iPhone's password, as its memory would be automatically cleared after ten wrong password attempts. The FBI relied on the All Writs Act of 1789 in asking Apple to create software that would enable the FBI to unlock the iPhone. The denial from Apple was based on the fact that the Communications Assistance for Law Enforcement Act (CALEA) II was not passed by Congress. Apple also cited United States vs. New York Telephone Co, the First Amendment, and stated that code was considered speech. The case was eventually dropped when a third party vendor was found to unlock the phone.

Another related case involved Philadelphia Police Officer Francis Rawls who was jailed in 2015 due to contempt for failing to decrypt two hard drives (thought to contain child pornography) taken from his home, claiming he did not remember the passwords. This was challenged under the fifth amendment rights against self incrimination, implying that producing the password would be the same as admitting that he owned the hard drive. The Third Circuit Court of Appeals rejected this argument saying that the court had ample evidence and giving the password would not give new information, and the information on the hard drive was not considered testimony. Rawls remained in jail for more than four years without being charged with a crime. He was finally released on appeal based on the fact that there is an 18-month cap on imprisonment for civil contempt.

A similar password case concerned using Touch ID to unlock a phone. Paris Hilton's iCloud storage was hacked, and a seizure warrant was granted for the "fingerprint on iPhone device" owned by Paytsar Bkhchadshyan in Los Angeles. Authorities were to "depress" her fingerprint on the sensor. The defense claimed 5th amendment protection but this was overruled by the court.

The Florida Court of Appeals Second District also ruled on granting a password in a case of indecent photographs against Aaron Stahl. Initially, a judge stated that the defendant cannot reveal the passcode (citing the constitution), but the decision was reversed by the Florida Court of Appeals Second District based on "self-incrimination" because the "passcode is not related to any criminal photos or videos found on the phone." The judge cited a case from 1988, Doe vs. U.S., where an accused person may be "forced to surrender a key to a strongbox containing incriminating documents but cannot be compelled to reveal the combination to his wall safe, illustrating the court's view on a potential difference between fingerprint and passcode. In a similar case, The State of Minnesota vs Diamond, a fingerprint was needed to unlock a phone in a burglary case. Diamond refused while asserting fifth amendment rights, but violations were denied and the phone was unlocked. In order to avoid 5th amendment concerns, the court had to introduce inculpatory evidence unrelated to the contents of the cellphone.

This issue remains an ongoing battle between tech companies and prosecutors, and was even the basis of a Congressional hearing. As recently as December, 2019, Apple continued to battle the FBI on privacy rights. In that case, a Saudi Air Force Officer killed three Americans at US Naval Base, in an act of terrorism, and attempted to break and discard two iPhones. The FBI could reassemble the iPhones, but could not access their contents. Apple maintained that it would not help create a backdoor, stating "Americans do not need to choose between weakening encryption and solving investigations." Law enforcement agencies continue to battle Apple and other technology companies over encryption as case law, legislation, and technology all continue to evolve.

6. Existing Training and Reference Resources

At the federal level, the Federal Judicial Center provides a number of resources to federal judges including orientation training, workshops, videos, conferences, and best practice documents covering various aspects of the work done by judges. These instructional resources in some cases address the impacts of technology and cyber forensics (Federal Judicial Center, n.d.). For example, the FJC conducts special focus programs. One example is the 'Search and Surveillance Warrants in the Digital Era', a seminar that in part addresses digital search technologies. The FJC also conducts targeted workshops like the National Workshop for U.S. Bankruptcy Judges that holds sessions on cybersecurity, discovery and e-discovery, and specialized uses of technology. These offerings are in addition to general training such as the Phase 1 & Phase 2 Orientation Seminar for Newly Appointed District Judges.

There are limited training requirements and opportunities for state judges. For example, in New Jersey training is limited to a two-and-a-half-day orientation and a two-and-a-half-week basic training course. However, states are recognizing the educational need and have advanced requirements as part of state court systems and procedures as well. In 2012, the American Bar Association changed the 'Model Rules of Professional Conduct' to include a technology competency requirement. Since this change, a majority of states have adopted the duty of technology competence as part of their state conduct policies. California has taken the recommended change further. In 2015, the State of California issued formal opinion 2015-193 that implements an ethical duty of competence pertaining to e-discovery including the discovery of ESI. In California, "an attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality" (The State Bar of California Standing Committee on Professional Responsibility and Conduct, 2015). In 2017, Florida became the first state to mandate technology continuing legal education credits for attorneys (O'Connor, 2017). North Carolina has followed suit requiring a similar requirement starting in 2019.

This trend of growing demand for training and education for judges and attorneys alike has pushed the need for resources to educate, train and assist this group. Across several states, a bench book may be provided to judges addressing various issues surrounding digital forensics. For example, the 'Bench book For New York State Judges Pertaining to the Discovery of Electronically Stored Information (ESI)'

provided by the New York Unified Court System's E-Discovery Working Group serves as a resource to state judges to "assist them in management of cases involving the discovery of ESI" (New York State Unified Court System's E-Discovery Working Group, 2015).

In Arizona, the Workgroup identified a three-pronged approach to educating judges across the state. In addition to multi-day conferences on forensic sciences, the state has implemented required training modules on forensic science in general for all new judges addressing the challenges judges may expect to see in a courtroom (Thumma & Wildeman, 2017). Additionally, the workgroup has established a dynamic forensic science reference page accessible only to judges providing a repository of reports, legal opinions and other materials that is updated frequently to handle the issue of rapidly advancing technology that a static bench book may otherwise be unable to address (Thumma & Wildeman, 2017). This approach provides flexibility and adaptability to the ongoing changes in forensics sciences.

A variety of resources provide federal, state and local court systems necessary references for displaying, analyzing and reviewing information. A non-exhaustive list of samples of those types of resources are outlined in the table below.

Table 1: Federal, State and Local Resources on Cyber Forensics and ESI[2]

Resource Type	Resource Name	Description
Book	Arkfeld's Best Practices Guide for ESI Pretrial Discovery – Strategy and Tactics	"This Guide is meant to be used in conjunction with the Electronic Discovery and Evidence (4th ed.)." The purpose of the… guide is to offer guidance and recommendation to legal professional s regarding pretrial strategy in discovering and disclosing (ESI)."
Book	Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials	"First published in February of 2016. The first edition attempted to be a 'comprehensive' collection of representative case law and related materials. Later editions followed that updated the first. This new edition consolidates everything into one compilation and adds additional case law and materials."
Checklist	EDiscovery Checklist: Admissibility of ESI at Trial	Checklist on the admissibility of ESI in the State of Minnesota.
Database	Electronic Discovery Case Database	"K&L Gates maintains and continually updates a database containing more than 3,000 electronic discovery cases collected from state and federal jurisdictions around the United States."
Database	The Simplified E-Discovery Case	"A collection of simple, easy to understand

[2] The resources presented are meant to be illustrative. The authors do not advocate the use of any particular resource.

	Law Library	analyses and resources on e-discovery case law."
Dissertation	Judges' Awareness, Understanding, and Application of Digital Evidence	"This study addressed judges' awareness, knowledge, and perceptions of digital evidence, using grounded theory methods."
General Resource	American Bar Association (ABA)	"At-a-Glance Tool for Information on E-Discovery"
General Resource	Federal Judicial Center	"The Federal Judicial Center is the research and education agency of the judicial branch of the U.S. government."
Guide	Criminal E-Discovery	"This pocket guide was developed to help judges manage complex e-discovery in criminal cases."
Guide	EDRM Identification Guide	Guidance outlining the identification phase of the EDRM model.
Guide	Guidance for the Provision of ESI to Detainees	"we believe that the provision of ediscovery to pretrial detainees… will also result in greater efficiency, reduced delay, and cost savings for the entire criminal justice system. We believe that facilities must necessarily transition to enabling pretrial detainees to review e-discovery, but we also recognize systemic institutional reasons,… why this evolution from paper-based review to e-discovery review will take time to implement… we have developed some practical guidance for jurisdictions to address the specific challenges in delivering e-discovery in digital format."

Guide	Managing Discovery of Electronic Information: A Pocket Guide for Judges	"This pocket guide is designed to help federal judges manage the discovery of electronically stored information (ESI)."
Journal Article (via ABA)	How Arizona Developed and Used a Needs Assessment to Guide Judicial Forensic Science Training	"provides an overview of… needs assessment… and the responses received from Arizona's judicial officers… describes programming at the December 2016 Arizona Judicial Forensic Science Conference, provides a summary of forensic science training added to the judicial training program, and offers an outline of the forensic science webpage created as a result of the efforts..." Provides toolkit for other states.
Library	National Software Reference Library (NSRL)	"Designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations."
Training	National Computer Forensic Institute	"Courses are designed for Prosecutors and Judges to effectively prosecute and preside over cases involving digital forensic evidence."
Webinar	Understanding eDiscovery in Criminal Cases: eDiscovery Best Practices	Multi-part webinar series addressing the issues and an overview of eDiscovery best practices.

7. Recommendations

1. Provide at least a brief cyber forensics overview and pointers to resource materials during orientation and training sessions for new judges. Depending on the training opportunities available, this could include a one-hour overview during orientation (which, for example, in New Jersey is a total of two and a half days), a one-day session during basic training (which runs for two and a half weeks in New Jersey), an appropriate time slot for federal "baby judge" training and subsequent deeper dives (perhaps on an elective basis) during future training sessions.

2. Provide online access for all judges to a database of rulings related to cyber forensics that is continually updated. See, for example, Arizona's dynamic forensic science reference page cited in Section 6. The database can be complemented by pointers to resources such as those given previously in Section 6, Table 1.

3. Include brief introductions to the following topics in training sessions for new judges and develop in-depth courses in these topics for advanced training. The advanced training courses would ideally include presentations from science and technology experts as well as legal experts:
   - Cyber forensics standards and procedures
   - How technological advancements affect standards
   - Electronically stored information (ESI)
   - Evolving legislation
   - Encryption and passwords

8. Conclusions

Rapid evolution of information and communications technology in everyday societal use means that the applicability of the current court standards of Daubert and Frye for cyber forensics cannot be sustained. The current NIST ISO17025 standard is also inappropriate for the cyber forensics field and therefore the approach to obtaining and ruling on the admissibility of evidence in the court system needs to continue to adapt. That the court system must remain flexible and adaptable regarding cyber forensics standards is the primary conclusion.

The lack of a concise approach to cyber forensics within the court system is increasingly proving the need for judges to have some basic knowledge in cyber forensics to effectively mediate the concerns of prosecutors and defense attorneys. This education and training requirement will not only allow judges to fundamentally understand cyber forensics but provide them the basis for appropriately dealing with electronically stored information (ESI) during the discovery process.

Most states offer judiciary colleges for new judges and there are requirements for continuing legal education. A module on cyber forensics within the judicial college and annual seminars, conferences and training may provide enough baseline knowledge that judges can bring into the courtroom limiting

bias and inadvertently bringing personal knowledge about technology into proceedings. As recommended by Kessler (2010), this baseline training would be applicable across all levels and types of courts. The training may be even more important at the local levels to limit constitutional challenges related to cyber forensics from being brought to higher-level courts. Placement within the current judiciary training approaches is the ideal fit.

Legislatively, movement on providing the courts with flexibility has already begun (O'Neill, 2018). Attorneys and judges in particular fields will need to continually review U.S. law while maintaining constant awareness of international laws and their impacts. The resources provided here are not exhaustive but can comprise an initial step into understanding the potential impacts as well as potential tools to address issues related to cyber forensics that will arise in the near future within the court room.

9. Works Cited

Arizona Task Force on Court Management of Digital Evidence. (2018). Report and Recoomendations of the Arizona Task Force on Court Management of Digital Evidence. *Washington Journal of Law, Technology & Arts, 13*(2), 166-201.

Austin, D., & O'Connor, T. (2018, January 11). Important eDiscovery Case Law Decisions of 2017 and Their Impact on 2018. Retrieved January 17, 2020, from https://cloudnine.com/webcasts/webcast-important-case-law-january-2018/

Bolch Judicial Institute, Duke Law. (2019). *Technology Assisted Review (TAR) Guidelines.*

Broughel, K., Worthington, J., Barnett, T., & Ehmke, A. (2018, December 13). *Proportionality and Technology Assisted Review—The Evolving Post-Amendment Landscape.* Retrieved January 17, 2020, from Paul Hastings: https://www.paulhastings.com/publications-items/details/?id=7d7d196c-2334-6428-811c-ff00004cbded#_ednref20

Chang, E. K., & Yoon, A. H. (2005). Does Frye or Daubert Matter? A Study of Scientific Admissibility Standards. *Virginia Law Review, 91*, 471-513. Retrieved from https://ir.vanderbilt.edu/bitstream/handle/1803/6293/Does_Frye_or_Daubert_Matter.pdf?sequence=1

Dixon, L., & Gill, B. (2002). Changes in the standards for admitting expert evidence in federal civil cases since the Daubert decision. *Psychology, Public Policy, and Law, 8*(3), 251-308. Retrieved from https://doi.org/10.1037/1076-8971.8.3.251

Federal Judicial Center. (n.d.). *Programs and Resources for Judges*. Retrieved June 2020, from Federal Judicial Center: https://www.fjc.gov/education/programs-and-resources-judges

Garrie, D. B. (2014). Digital Forensics in the Courtroom: Understanding Content and Quality. *Northwestern Journal of Technology and Intellectual Property, 12*(2), 121-128. Retrieved from http://www.nmid.uscourts.gov/documents/districtconference/2014/garrie/Digital%20Forensic%20Evidence%20in%20the%20Courtroom-%20Understanding%20Content.pdf

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2014). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence.* RAND Corporation. Retrieved from National Criminal Justice Reference Service.

Hedges, R. J., Rothstein, B. J., & Wiggins, E. C. (2017). *Managing Discovery of Electronic Information: A Pocket Guide for Judges - Third Edition.* Washington, D.C.: Federal Judicial Center. Retrieved June 26, 2020, from https://www.fjc.gov/sites/default/files/materials/38/Managing%20Discovery%20of%20Electronic%20Information_Third%20Edition_Second%20Printing_2019.pdf

Henry, K. A., & Palacios, D. (2015, October 26). *The 2015 Amendments to the Federal Rules of Civil Procedure: Changing the Way Civil Litigants Operate in Federal Court*. Retrieved January 17, 2020, from medialawmonitor: http://www.medialawmonitor.com/2015/10/the-2015-amendments-to-the-federal-rules-of-civil-procedure-changing-the-way-civil-litigants-operate-in-federal-court/

Henseler, H., & van Loenhout, S. (2018). Educating judges, prosecutors and lawyers in the use of digital forensic experts. *DFRWS 2018 Europe - Proceedings of the Fifth Annual DFRWS Europe* (pp. S76 - S82). Elsevier Ltd. Retrieved from http://www.dfrws.org/file/946/download?token=b13T1HMA

Hill, J. L. (Ed.). (2019, July 9). *The States of Daubert after Florida*. Retrieved January 17, 2020, from LexVisio: https://www.lexvisio.com/article/2019/07/09/the-states-of-daubert-after-florida

Joint Working Group on Electronic Technology in the Criminal Justice System. (2012). *Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases.* Department of Justice (DOJ).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology.* U.S. Department of Commerce. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Kessler, G. C. (2010). Judges' Awareness, Understanding, and Application of Digital Evidence. Florida. Retrieved January 17, 2020, from https://www.garykessler.net/library/kessler_judges&de.pdf

logikcull. (2020, January 17). *An Introduction to eDiscovery*. Retrieved from logikcull: https://www.logikcull.com/guide/introduction-to-ediscovery-basics

McDonough, S., & Jacqueline, B. (2018, October 25). *Frye Is Now, and Once Again, the Standard for Expert Opinion Admissibility in Florida*. Retrieved January 17, 2020, from Product Liability Advocate: https://www.productliabilityadvocate.com/2018/10/frye-is-now-and-once-again-the-standard-for-expert-opinion-admissibility-in-florida/

National Forensic Science Technology Center. (2013). *A Simplified Guide to Forensic Evidence Admissibility & Expert Witnesses.* Retrieved from A Simplified Guide to Forensic Science: http://www.forensicsciencesimplified.org/legal/702.html#:~:text=Federal%20Rules%20of%20Evidence%2C%20Rule,included%20rules%20on%20expert%20testimony.

New York State Unified Court System's E-Discovery Working Group. (2015). *Bench book For New York State Judges Pertaining to the Discovery of Electronically Stored Information ("ESI").* New York State Courts.

O'Connor, T. (2017, December). eDiscovery and the GDPR: Ready or Not, Here it Comes. Retrieved January 17, 2020, from https://cloudnine.com/ediscoverydaily/electronic-discovery/ediscovery-gdpr-ready-not-comes-part-four-ediscovery-best-practices/

One Hundred Fifteenth Congress, Committee on the Judiciary. (2017, December). *United States Courts.* Retrieved from Federal Rules of Evidence: https://www.uscourts.gov/sites/default/files/evidence-rules-procedure-dec2017_0.pdf

O'Neill, M. (2018, January 28). *Streamlining the Admissibility of ESI: Amendments to Federal Rule of Evidence 902*. Retrieved from DiscoverReady.com: https://discoverready.com/news-insights/insights/streamlining-admissibility-esi-amendments-federal-rule-evidence-902/

Sadiku, M. N., Tembley, M., & Musa, S. (2017). Digital Forensics. *International Journal of Advanced Research in Computer Science and Software Engineering, 7*(4), 274-276. Retrieved from https://www.researchgate.net/profile/Mahamadou_Tembely/publication/318665422_Digital_Forensics/links/5b10bab8a6fdcc4611d983a6/Digital-Forensics.pdf

Scientific Working Group on Digital Evidence. (2018). *SWGDE Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis.* SWGDE.

Sommer, P. (2018). Accrediting digital forensics: What are the choices? *Digital Investigation*, 116-120. Retrieved from https://www.sciencedirect.com/science/article/pii/S1742287618301701

Sullivan, C. C. (2018, January 9). *New Discovery Rules Are Coming to Criminal Law*. Retrieved from logikcull: https://www.logikcull.com/blog/new-discovery-rules-are-coming-to-criminal-law

The State Bar of California Standing Committee on Professional Responsibility and Conduct. (2015). *The State Bar of California Standing Committee on Professional Responsibility and Conduct Formal Opinion No. 2015-193.* Retrieved January 17, 2020, from catalystsecure.com: https://catalystsecure.com/components/com_wordpress/wp/wp-content/uploads/2015/08/CAL-2015-193-11-0004-06-30-15-FINAL.pdf

Thumma, S. A., & Wildeman, J. (2017). How Arizona Developed and Used a Needs Assessment to Guide Judicial Forensic Science Training. *The Judges' Journal, 56*(4), 29-32. Retrieved from https://search.proquest.com/openview/d533ac12217a2248761466c3e187123c/1?pq-origsite=gscholar&cbl=12816

10. Acknowledgements

We would like to thank The Honorable Ronald Hedges, currently Senior Counsel at Dentons. Ron, a United States Magistrate Judge in the United States District Court for the District of New Jersey from 1986 – 2007, met with us and provided ideas, feedback, and editing for early drafts of this white paper. He also enlisted the help of several judicial colleagues for the editing and feedback process for which we are very grateful. We would also like to acknowledge the judges, attorneys, prosecutors, and law enforcement officers we interviewed for this white paper. While we will not specifically mention them by name, the information and insights they provided were invaluable and are incorporated throughout the paper.