THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 14 | Number 4 Article 3

April 2020

Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration

Martin Novak
National Institute of Justice, martin.novak@usdoj.gov

Recommended Citation

Novak, Martin (2020) "Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration," *Journal of Digital Forensics, Security and Law*: Vol. 14 : No. 4 , Article 3.
DOI: https://doi.org/10.15394/jdfsl.2019.1609
Available at: https://commons.erau.edu/jdfsl/vol14/iss4/3

DIGITAL EVIDENCE IN CRIMINAL CASES BEFORE THE U.S. COURTS OF APPEAL: TRENDS AND ISSUES FOR CONSIDERATION

Martin Novak
National Institute of Justice
martin.novak@usdoj.gov

1. INTRODUCTION

Though the use of computer forensics in criminal investigations has expanded in recent years, there is little empirical evidence about the prevalence of the use of digital evidence in the court system and its impact on prosecutorial outcomes. [1]

The terms digital evidence and computer forensics are closely related, yet there are differences. Computer forensics is the uncovering and examination of evidence located on all electronic devices with digital storage, including computers, cell phones, and net-works. Though there is no universally accepted standard for computer forensics, there are generally accepted practices in place. [2] In 2014, the Scientific Working Group on Digital Evidence (SWGDE) published its Best Practices for Computer Forensics to describe the best practices for collecting, acquiring, analyzing, and documenting the data found in computer forensic examinations. Similar to other published best practices, it is not a step-by-step guide nor legal advice, and only addresses the types of technologies available at the time of publication.

While computer forensics involves all digital storage, digital evidence is information stored or transmitted in binary form that may be relied on in court. There are countless potential sources of digital evidence, including text messages, images downloaded to a computer, a mobile device's call log, network access logs, chat sessions, internet browser history and cache files, passwords, documents, spreadsheets, and databases.

This paper is an examination of federal criminal cases before the United States Court of Appeal in which legal issues were related to digital evidence. The purpose of this research was to determine the most common legal basis for appeals relating to the introduction or exclusion of digital evidence, the frequency with which cases involving an appeal regarding digital evidence affirmed or reversed for the defense, whether certain challenges to digital evidence are more prevalent than others, and whether there are trends or areas of the law as applied to computer forensics and digital evidence needing further attention by the criminal justice system.

The digital evidence produced by computer forensics has the potential to identify suspects, win acquittal, or obtain a convic-

tion. Information obtained through digital evidence can be used to both corroborate and establish necessary elements of prosecution and defense cases such as motive, suspect or witness location, and alibis. Two high-profile cases anecdotally illustrate both the value of introducing digital evidence, as well as the limited value of that evidence in the absence of clarity and credibility of the forensic methods used to obtain it.

1.1 Cobb County, Georgia

On September 14, 2014, Ross Harris was charged with two counts of felony murder in the death of his son, Cooper Harris. The Cobb County, Georgia charging documents stated that Harris maliciously caused the death of his son by leaving him alone in a hot motor vehicle with the windows shut on June 18, 2014. [3] He was also charged with Criminal Cruelty to a Child and Criminal Attempt to Commit a Felony.

Investigators were at first puzzled as to why a seemingly loving father would murder his child. A forensic examination of a computer, mobile device, thumb drive, external hard drive, SD card, and DVD – all belonging to Harris – led police to discover the motive for the murder. Text messages recovered from the computer showed that Harris was having an affair with a 17-year-old high school student. Online searches recovered from his computer demonstrated that Harris was searching for information on the age of consent in the State of Georgia and "how to survive in prison." Examination of his mobile device also recovered evidence that Harris had been "sexting" with several other women while his son was dying in the overheated car. On November 14, 2016, Harris was convicted of murder in the first degree of his son and sentenced to life without parole.

According to the American Bar Association, digital evidence "can have a long-lasting effect on the court or jurors, regardless of the reason for being admitted into evidence and notwithstanding any related jury instructions as to the limitations of that evidence." [4] The kind of effect may depend on the quality of the evidence presented. Matt McCusker, of the American Society of Trial Lawyers, warns that "the average juror does not have the expertise to differentiate between 'good science' and 'junk science,' so the court must help them by excluding dubious evidence." [5] The murder trial of Casey Anthony, outlined below, is a case in point.

1.2 Orange County, Florida

On October 14, 2008, Casey Anthony was indicted by an Orange County, Florida grand jury with Capital Murder in the First Degree in the death of her daughter, Caylee Anthony. Prosecutors alleged that Anthony used chloroform on Caylee, then suffocated her by covering the girl's mouth and nose with duct tape. They also alleged that Anthony put her daughter's body in her car trunk before disposing of it. The child's skeletal remains were found in December 2008, less than a mile from the home of Anthony's parents.

A computer forensics examiner testified for the prosecution, stating that someone had searched the words "chloroform" a total of 84 times on a computer seized from the Anthony home. [6] The examiner further testified that the searches were found in a portion of the hard drive believed to have held deleted files. The implication was that Anthony had made those searches and was evidence of premeditation.

During his forensic examination of the computer, the examiner used two tools to perform the keyword searches that found the word "chloroform." While it is generally good forensic practice to duplicate one's searches with multiple tools, in this case, it caused confusion for the jury. The timestamps, which indicate when a particular search was made, did not synch between the two tools used.

This could have easily been explained in that the tools used different methods to conduct their respective searches, but the prosecution gave no such explanation.

The counsel for the defense saw a weakness in the prosecution's case and swiftly brought it to the jury's attention. Jose Baez, lead counsel for the defense, stated, "The state's computer forensic evidence involving chloroform research, a central element of their premeditation argument, was used to mislead the jury and that the flaws in that evidence infected their entire case like a cancer." [7]

Anthony was found not guilty on the charge of capital murder in the first degree on July 5, 2011. The jury based its decision, in part, on the lack of credible forensic evidence linking her to the alleged crime.

These two cases clearly illustrate the power that digital evidence can have in the disposition of a case, and raise questions about the legal precedent regarding digital evidence and its impact on prosecutorial outcomes. The next section discusses relevant literature that has helped inform the debate about computer forensics and digital evidence.

2. LITERATURE REVIEW

Although the literature on computer forensics is somewhat limited, particularly in regard to courts, there is research that discusses issues relevant to computer forensics and digital evidence in courts. This literature can be largely be broken into the three areas of Search and Seizure, Admissibility, and Precedent. Together, the literature under each topic forms a foundation of research on which the research questions of this study were built. In this literature review, each body of literature is discussed.

2.1 Search and Seizure

Search and seizure allows law enforcement to search and seize property after obtaining a warrant based on probable cause. In considering the prevalence and impact of computer forensics in the court system, it is important to consider digital evidence regarding search and seizure practices. Because it is inherently different from physical evidence, digital evidence presents a unique set of search and seizure complications.

As Garfinkel states in Digital Forensics, electronic storage devices can serve as two different kinds of digital evidence, each with its own set of complications. [8] In the first case, an electronic storage device might contain evidence of a crime that took place in the physical world, such as murder, rape, or child molestation. In these cases, the device is incidental to the crimeit is a vessel that helped facilitate a crime, but not an object directly involved in the physical criminal act. In this case, investigators face the difficulty that, as Garfinkel states, "Computerization has made the evidence harder for investigators to analyze than paper records." [9]

The second scenario in which an electronic storage device serves as a form of digital evidence is where it is inherently part of the crime committed. An example of this is hacking or possession of child pornography. In these cases, Garfinkel says, "investigators are often hampered by the technical sophistication of the systems and the massive amount of evidence to analyze." [10]

In both cases, the presence of digital evidence raises important questions about how search and seizure practices should be applied. This review examines the literature around these debates, particularly with regard to Warrants and Plain View.

2.1.1 Search and Seizure: Warrants

A warrant provides police with the legal authority to conduct a search of physical property. However, the concept of warrants was developed in and for a context of physical evidence, and its application to digital evidence is complicated. The Fourth Amendment protects against unreasonable search, but there is debate among scholars with regard to whether and how the rules for searching for digital evidence should be adapted so as not to violate this protection. This debate is outlined below.

The scholars Kerr (2005), Rummel (2011), and Bartholomew (2014) argue that the search for digital evidence is not a one-step process, as with physical evidence, but rather a two-step process. Kerr explains that "the police first execute a physical search to seize computer hardware, and then later execute a second electronic search to obtain the data from the seized computer storage device." [11]

Similarly, Ohm (2011) believes that a second warrant should be required in order to meet the particularity requirements of the *Fourth Amendment*. Ohm states that this warrant should "clearly approv[e] the search of a particular computer's hard disk or storage media, which is already secured and seized by the government pursuant to an earlier probable cause search (ideally a first warrant) . . . [ensuring that] when a magistrate approves that search, he or she is aware of what is being authorized." [12]

Other scholars have historically disagreed with this two-step view. Some have argued that computer searches should be viewed by the courts in the same manner as the physical search of documents and other containers of information, such as a filing cabinet. Clancy (2005) explains that "a computer is a container of containers of documents, that is, each individual file is a separate container — just like each manila file in a filing cabinet is a container — that requires a separate opening to determine what is inside." [13] Clancy states that accepting this view does not imply accepting that a particularized warrant will become a general warrant. Instead, the rules that are in place that limit the scope of the search itself, such as the nature of the crime or the evidence one expects to find, will allow the court to determine the sufficiency of the information provided to them in the warrant that authorized the search.

In 2015, the Supreme Court offered clarity with regard to the warrant requirement to search digital content. In Riley v. California decision [14], the Supreme Court declared that the "answer to the question of what police must do before searching a cell phone seized incident to an arrest is . . . simple — get a warrant." [15] [16] This landmark ruling closed a debate regarding whether law enforcement needed to obtain a warrant before searching for digital evidence.

Although the Supreme Court declaration established the need for a warrant, questions remained regarding the details of warrants used to collect digital data. Gershowitz (2015) suggests two approaches for searches involving cell phones. First, he says that "judges should impose search protocols that specify in advance exactly how police should execute warrants and sift through electronic data." [17] In a second method, Gershowitz suggests that "magistrates should initially restrict warrants to a manual search of the particular functions or applications for which there is probable cause." [18] He predicts that the use of these restrictions will protect the privacy rights of individuals, prevent the use of the "good faith" exception, [19] and allow law enforcement to conduct searches of cell phones when there is probable cause to do so.

Similarly to Gershowitz, Huynh (2015) suggests a process-based protocol for the search of cell phones in which forensic examiners

must describe the following in warrant applications: a technical explanation of the search procedure, an explanation of what is being sought, the extent of the process being used, description of the process used to copy the device for analysis, methods used to isolate information that is outside of the scope of the warrant, plans for purging nonresponsive data, and detail of the access control policies in place by the examining agency. [20] Huynh contends that the protocol would enhance the particularity within a search, and limit the number of successful defense challenges at trial.

An additional complication in the application of search and seizure principles to digital evidence relates to the problem of non-responsive digital data. In Commentary on the Ganias Case, Kerr (2015) discusses a way to avoid the problem of over-seizure and the disposition of non-responsive data. In the case of paper records that have been seized, once the non-responsive records have been filtered, they can easily be returned. This is not the case with records that exist on digital media because "[w]e cannot cut off a piece of the physical hard drive. Even if we could, data is not stored contiguously on the medium." [21] It is simply not possible to return non-responsive data in a computer search. This leads to the concern that law enforcement will use initially non-responsive data as grounds for future searches unrelated to the initial search warrant. Kerr's solution is to forbid law enforcement from obtaining a second warrant based on non-responsive data found in the first warrant. To use the non-responsive data, Kerr says, "The exclusionary rule would not apply if the government searched the seized computer under a second warrant when it could prove by a preponderance that the evidence sought in the second warrant would have been obtained elsewhere." [22]

2.1.2 Search and Seizure: Plain View

Closely related to the issues of warrants in collecting and searching digital data is the issue of the Plain View Doctrine. In a context of physical evidence, plain view allows a law enforcement officer to search items found in plain sight without a warrant. However, the definition of plain view is complicated in the context of digital evidence.

Because inculpatory evidence can be hidden, obfuscated, or encrypted, law enforcement regularly receives authorizations to seize large amounts of data. This leads to concerns of over-seizure, and complicates the definition of plain view once data is in the hands of law enforcement. Angeli et al. (2005) state that the "seizure and search of electronic data presents unique challenges and illustrates the tension between the legitimate law enforcement need to search for and seize evidence, on the one hand, and the Fourth Amendment privacy interests of individuals and other entities, on the other." [23]

The literature presents several views on the debate of how the concept of plain view should apply to digital evidence. Some scholars believe that plain view in the traditional sense should apply to computer searches. [24] Mantei (2011) states that the "scope of plain view seizure, like the search itself, is dictated by the factual circumstances of an investigation." He also advises that law enforcement should seek a second warrant when evidence is discovered that is not part of the original warrant. Hood (2011) says that "the inadvertent discovery requirement in the context of plain view seizures of electronically stored evidence offers the most viable method for ensuring that government seizures of electronically stored evidence do not become general or exploratory and comply with the explicit commands of the Fourth Amendment." [25]

Another line of thought among scholars is that the forensic examination of computers should be excluded from the plain view doctrine. Their reasoning is that some potential evidence on a computer may not be discoverable without the use of specialized tools, such as the contents of a computer's memory, metadata, the internet cache, deleted files, password protected files, file fragments, and files in unallocated space. This evidence will never be in plain view. For these reasons, Daniel (2009) concludes that a "targeted forensic examination should be completely excluded from the plain view doctrine as it is an intrusive search and allows the examiner to see everything on the computer, regardless of its location or origin." [26]

A third opinion, expressed by Weinstein and Drake (2014), is that the federal wiretap stat-utes could be applied to computer searches, thereby protecting the privacy of individuals and the investigative needs of law enforcement. Wiretap orders function much like search warrants, except they allow for the collection of information as it occurs in real time (such as phone conversations). There are a series of procedures that the government must follow if wiretapping. These procedures are designed to minimize privacy challenges, and require the government to minimize the interception of non-criminal conversations, report information seized to the judge within 14 days of authorization, and be subject to ongoing monitoring by the presiding judge. Applying these wiretap protocols to computer searches would be a "model for consistent procedures and judicial oversight." [27] Employing these protocols could even provide an incentive for law enforcement to conduct searches more efficiently, knowing that the protocols for reporting are in place.

2.2 Admissibility

The second body of literature relevant to questions of digital evidence and courts discusses the issue of admissibility. To be considered in court, evidence — physical or digital — must pass the test of admissibility, which includes consideration of whether the evidence is relevant, reliable, and not unfairly prejudicial. Givens (2004) points to major differences between electronic and paper evidence that should be addressed when consid-ering admissibility, using email for his examples. The first difference is obtainability. Givens points out that "without email, many conversations simply would not exist." [28] The second difference is one of availability. Email often passes through and is stored by third-party systems, such that "a simple search of the third party system could turn up several 'deleted' or otherwise misplaced files." [29] Finally, there is a difference in the content of an email versus a paper document. Email contains information not found in pa-per documents, such as file header information, distribution lists, and receipts of acknowledgment. With this knowledge, Givens says, those offering email as evidence "should at least be required to present witness testimony to show the reliability of the computer system used to store or create the electronic data being offered." [30]

In Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. May 4, 2007), [31] Magistrate Judge Paul D. Grimm (United States District Court for the District of Maryland) provided the field with guidance on the admissibility of electronic evidence. In the ensuing years, the case drew comments and criticism from legal scholars. According to the court, when Electronically Stored Information (ESI) is offered as evidence, the following evidentiary rules must be considered: relevancy, authenticity, hearsay, best evidence, and probative value. [32]

Levy-Sachs and Archambault (2008) stated that "[D]espite the fact that the Court provides a general roadmap for admissibility of ESI, the Court does not indicate whether

more stringent standards are necessary or desirable." [33] Frieden and Murray (2011) believe that the methods for authentication proscribed in Lorraine v. Markel are similar to those of traditional evidence. They state that though "certain issues, such as authentication, may be more complicated in the context of electronic evidence, traditional evidentiary principles can be consistently adapted to address questions regarding the admissibility of electronic evidence." [34]

In an article written for the American Bar Association, Grimm, the presiding judge in the Markel case, recognizes that some courts subject electronic evidence "..to far greater levels of scrutiny than applied to non-digital evidence when deciding whether to admit it." [35] He provides advice for those who consider submitting digital evidence at trial: "If you identify the digital evidence you want to use prior to trial, learn as much as possible about how it works (using the Internet can be an inexpensive and helpful way to do so), carefully select which authentication method you want to use, and (if it involves using an expert or subpoenaing records) make arrangements sufficiently far in advance to be prepared at trial, you will greatly enhance your chances of success." [36]

2.3 The Daubert Standard

The Daubert Standard requires that the five factors of testing, peer review, error rate, standards, and acceptability be applied to scientific evidence. The Daubert Standard was promulgated in the landmark Daubert v. Merrell Dow Pharmaceuticals, 579 U.S. 92 (June 28, 1993), which establishes the aforementioned standard for admitting expert scientific testimony in federal court. This ruling was further expanded in Kumho Tire Co. v. Carmichael, 119 U.S. 1167 (Mar. 23, 1999) [37], which established that the Daubert standard must be applied to expert testimony from non-scientists.

Legal scholars have since weighed in on the Daubert Standard as it applies to digital evidence as well as the expert witnesses that testify on that evidence. Meyers and Rogers (2004) wrote of the need for standards and certification in the field of computer forensics. One area of concern noted was the inability to know the exact functionality of the tools used in computer forensics. Their observation that the "majority of the tools and software used in computer forensics is proprietary and copyrighted, thus negating the ability to access the source code" [38] is still valid today. They also noted a lack of known error rates for these same tools. They conclude that, much like a certified professional accountant, the field of computer forensics needs methods that "ensure that the practice is credible and reliable and that the individuals claiming to be professionals have met a certain certification criterion." [39] In their conclusion, Meyers and Rogers warn that the "continued lack of a professional certification, investigative standards, and peer-reviewed method, may ultimately result in computer forensics being relegated to a "junk science," as opposed to a recognized scientific discipline." [40]

Atkinson similarly argues for the need to validate data. According to him, the means to produce digital evidence are software programs, for which formal proofs are virtually nonexistent. These programs are themselves a sequence of binary digits and are subject to frequent changes in their code. This leads to Atkinson to ask: "At what point should a mess of ones and zeroes be trusted either as evidence, or to provide it?" [41] To address these concerns, Atkinson contends that software engineers should promote transparency in the "inner workings" of the tools that produce digital evidence, providing more opportunities for validation of tools, and provide the tools more credibility in court.

Garfinkel (2010) also grappled with the lack of known error rates in the field of computer forensics, noting that the "research community should work to develop digital forensic techniques that produce reportable rates for error or certainty when they are run." [42] Garfinkel also notes the benefit to tool developers and those evaluating tools for use in having a standardized set of digital corpora. This would enable developers to test their tools with larger data sets and allow others to replicate their results more easily.

The Daubert Standard also applies to testimony of expert witnesses, Garrie and Morrissy (2014) suggest that a well-written computer forensic report could circumvent the need for an expert's testimony altogether. According to the authors, the adequately written report should sufficiently detail the methods used, document the assumptions made by the computer forensic examiner, the tools used to complete the forensic exam, eliminate any superfluous information, and be objective in its tone. Finally, the findings in the report "should be qualified in regard to the capabilities of the [computer forensics] tool used in the exam, and the scope of the investigation." [43]

2.4 Precedent

The American legal system relies heavily on the doctrine of stare decisis, which means to stand by things decided. In an examination of Supreme Court cases from 1946 through 1995, Spriggs and Hansford (2001) found that "a precedent is more likely to be overruled when it is ideologically incongruent with the preferences of a subsequent Court." [44] In other words, conservative precedents are more likely to be overruled by liberal courts.

Benesh and Riddick (2002) examined precedent and circuit characteristics to determine whether a circuit court was likely to follow Supreme Court precedence. The factors in their analysis included the unanimity of the precedent ruling, the complexity of the matter ruled upon, and the age of the precedent being overruled. Their results showed that the circuit courts complied with the overruling of older precedents more quickly than more recent precedents. However, those same circuit courts "were more reluctant to comply with new criminal procedure precedents than they were precedents in other areas." [45]

Kassow, et al. (2012) examined the responsiveness of state supreme courts to precedents set by the U.S. Supreme Court. Their methodology included scrutinizing the treatment of those precedents in the state court's opinions to test the value of precedent strength versus the influence of the ideological preferences of the state courts. [46] They found that the "more the U.S. Supreme Court reinforced its original precedent with subsequent decisions indicating continued support for the precedent, the more likely state courts were to provide a positive treatment of the precedent." [47]

Re (2016) found that the lower courts may apply more narrow readings of the federal court's precedent. He called this action "narrowing from below." There are several reasons lower courts may narrow from below, including "to update obsolete precedents, mitigate the harmful consequences of the Court's errors, and enhance the transparency of their decision-making process." [48] He cites the following legitimacy conditions that lower courts consider when narrowing from above: whether the precedent applies, whether it is correct, and whether it implicates other legal principles. Re concludes that "narrowing from below is usually legitimate when lower courts adopt reasonable readings of higher court precedent, even though those readings are not the most persuasive ones available." [49]

Alan Butler discusses how the precedent set in Riley v. California, (134 S. Ct. 2473.

2014), may affect how lower courts rule on the issue of how long law enforcement may collect, search, and store digital data. Butler begins by pointing out that Riley precedent "supports the conclusion that the retention of electronic data should be subject to different Fourth Amendment rules than those used for handling physical evidence, [and that] Riley would also support a narrower construction of the 'plain view' exception for digital searches." [50] He then demonstrates how the Riley precedent may be interpreted by the lower courts.

In United States v. Ganias, (F. App. 9706 2nd Cir. 2016), Butler finds that the Second Circuit's ruling that "the government's 'seizure and retention' of digital files beyond the scope of their 2003 warrant was unreasonable under the Fourth Amendment" [51] was consistent with the privacy interests expressed in Riley, and that other courts would likely follow precedent in this regard.

In United States v. Miller (34 F. Supp. 3d 695), Butler found that the Third Circuit rejected the defendant's argument that a forensic search of his digital camera violated his rights under the Fourth Amendment. In this in-stance, the court took a narrower view of Riley, saying that "the search of a digital camera is different than the search of a smartphone because cameras only 'contain a limited type of data, restricted to image and video files that do not touch the breadth or analysis" from a warrantless search incident to arrest.' [52]

Finally, Atkinson (2014) asserts that the advancement of technology occurs at a rate that leaves the legal system in a constant state of trying to catch up. According to him, the courts depend on precedent "set in wholly different contexts" that are "reliant on a digital forensics field still in its infancy." [53] While it is essential to review examples of precedent set in previous cases, we should also keep in mind that, as Atkinson argues, these precedents may have been set in a legal context that is no longer relevant.

Although the literature on the prevalence and impact of digital evidence in courts is some-what limited, the bodies of literature discussing Search and Seizure, Admissibility, and Precedent does provide a context for the research this paper undertakes. The existing literature forms the foundation on which the research questions of this study were built — allowing the researcher to ask questions of the prevalence and impact of digital evidence in courts.

3. METHEDOLOGY

3.1 Scope

The following analysis is based on a review of relevant criminal cases in the U.S. Circuit Courts of Appeal from 2010 through 2015. The United States circuit courts of appeal were an ideal sample for this study for two principal reasons. First, the 11 circuit courts of appeal and the associated 94 United States district courts cover the nation. There is at least one court in each state and the District of Columbia. Second, the 11 courts of appeals and the 94 district courts adhere to the same rules of evidence – the Federal Rules of Evidence. This is important when trying to compare across or between the 11 circuit courts of appeal.

3.2 Research Questions and Objectives

A retrospective study was used to answer the following research questions:

- What is the most common legal basis for appeals relating to the introduction or exclusion of digital evidence?
- How often are cases involving an appeal regarding digital evidence affirmed or reversed for the defense?

- What were the most frequently occurring legal grounds for reversed judgments for the defense when digital evidence is involved?
- What was the most frequently occurring legal ground for affirmed judgments for the defense when digital evidence is involved?
- Are some of the challenges to computer forensics and digital evidence more prevalent than others? If so, why?
- Based on the results of this study, are there trends or areas of the law as applied to computer forensics and digital evidence that need further attention?

3.3 Data and Search Terms Used

Data for this project was drawn from cases that were affirmed or reversed by the United States Courts of Appeal for the period 2010-2015. Cases were identified via LexisNexis, using the following search terms: Computer, Computer Forensics, Chat Log, Electronic Evidence, Cell Phone, Sexting, iPhone, Child Pornography, Digital Evidence, Computer Investigation, GPS, and Encryption. Data was compiled in a Microsoft Access database and analyzed using Microsoft Excel. [54]

3.4 Cases Excluded

While searching for cases, three categories of appeals became apparent: Search and Seizure, Evidence Presented at Trial, and Other Issues. The digital forensic process has three major components: Seizure, Acquisition and Analysis, and Reporting. From Figure 1, we can see that the three components of the digital forensic process line up quite well with the first two categories for bases of appeal: Search and Seizure and Evidence Presented at Trial. It is also apparent that the Other Issues category basis of appeals (i.e., Double Jeopardy, Prosecutorial Misconduct, Sentencing, etc.) have little to do with either the way the evidence was obtained, or how it was presented in court. For these reasons, appeals that were based on "other" issues were excluded from the results and analysis for this study.

4. RESULTS AND DISCUSSION

The search parameters mentioned above identified 145 appeals involving legal issues related to digital evidence heard by the United States Courts of Appeal for the period 2010-2015.

All of these appeals followed convictions for federal criminal offenses (see table 6 in appendices for types of criminal offenses prosecuted). The types of technology where evidence was discovered included desktop computers, laptops, GPS tracking units, mobile devices, and external storage devices. Of the 145 appeals included in this study, 138 appeals (95.17 percent) were either affirmed or reversed for the government. Seven appeals (4.83 percent) were either affirmed or re-versed for the defense. [55]

In a 2010 article in Judge's Journal, Clancy points out that nearly "70 percent of all re-ported appellate decisions involving the search or seizure of digital evidence are concerned with the recovery of child pornography." [56] In line with this finding, 89 percent of appellate decisions in this study were related to the search and seizure of digital evidence related to the recovery of child pornography.

Sufficiency of Evidence was the most frequently occurring legal issue encountered as a basis for appeal at 31.03 percent, followed by Probable Cause at 27.59 percent; Defective Warrants at 12.24 percent; and Defective Warrants at 12.41 percent. Other legal issues

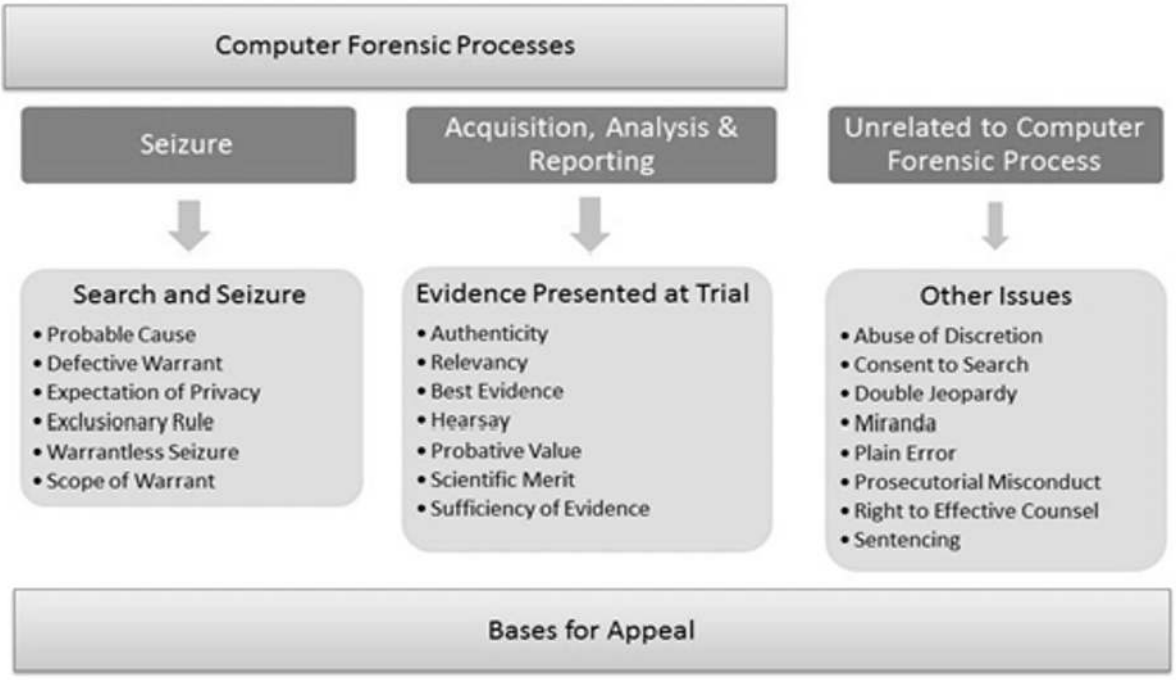

Figure 1. Digital Forensic Process Compared to Bases for Appeal

less frequently encountered included Scope of the Warrant, Probative Value, Expectation of Privacy, Scientific Merit, Exclusionary Rule, Relevancy, Authenticity, and Hearsay. A complete list of legal issues can be found in Table 2 of Appendix II.

4.1 Legal Issues

The United States District Court Systems adheres to the Federal Rules of Evidence (FRE), first adopted in 1975. [57] The rules regarding the introduction of digital evidence are similar to that of any other evidence produced at trial. The legal issues encountered within the 145 cases in this study were categorized as Search and Seizure, and Evidence Presented at Trial. Pertinent FRE Rules or precedent rulings, along with exemplar cases, are provided in the following sections that detail the legal issue argued on appeal, the reasoning of the court, and the outcome of the appeal.

4.1.1 Search and Seizure

Probable Cause Digital evidence produced at trial must have been obtained with a valid search warrant based on probable cause to search for evidence of a crime or criminal activity. The Fourth Amendment limits the ability of law enforcement agents to search for evidence. If probable cause cannot be demonstrated, then evidence will likely be suppressed under the Exclusionary Rule. This legal principle was first established by the United States Supreme Court in 1914 [58] when the court held that "evidence obtained by unconstitutional means cannot be used against a defendant." [59] Although val-id warrants have always been generally required by the courts, there are exceptions that allow law enforcement to engage in warrant-less searches. The exceptions include: Detention Short of Arrest: Stop-and-Frisk [60]; Search Incident to Arrest [61]; Vehicular Searches [62]; Vessel Searches; Consent Searches; Border Searches; "Open Fields" [63]; Plain View

[64]; Public Schools [65]; Prisons and Regulation of Probation [66]; and Drug Testing. [67]

In United States v. Schesso, 730 F.3d 1040 (9th Cir. Wash. 2013), the district court for the Western District of Washington appealed a district court ruling on the suppression of evidence gained from a search of the defend-ant's home. In ruling to suppress the evidence, the district court held that "the affidavit failed to connect generalized statements about child pornography collectors to Schesso, thus rendering the warrant facially deficient and the good faith exception inapplicable." [68]

The Ninth Circuit Court of Appeals reversed this decision determining that "because there was a fair probability that evidence of child pornography would be found on the defend-ant's computer system, the underlying facts supported a finding of probable cause; that the warrant was not overbroad and did not raise the risks inherent in overseizing that this court considered in United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010)." [69]

Defective Warrant Defective Warrant appeals tend to center on the notion of the staleness of the warrant. In general, "stale information cannot be used in a probable cause determination." [70] Yet, whether information in a warrant is stale is dependent in part by the inherent nature of the crime. For example, child pornography "is not a fleeting crime" and "is generally carried out in the secrecy of the home and over a long period." [71] The staleness of a warrant is difficult to prove with regard to child pornography because the pornography is stored on computers, may readily be duplicated, retained indefinitely, and may well be recovered by forensic software long after it has been deleted. [72]

In United States v. Hampton, 504 F. App. 402 (6th Cir. Nov. 5, 2012), Jack Eugene Hamp-ton appealed his conviction on charges of receipt of child pornography in violation of 18 U.S.C.S. § 2252(a)(2), and possession of child pornography in violation of 18 U.S.C.S. § 2252(a)(4)(B). In his appeal, Hampton argued that the affidavit used to obtain to search his residence was "stale because the warrant was executed more than ten months after German law enforcement officers observed child pornography shared through his IP address." [73]

The panel for the Sixth Circuit found that given "the nature of child pornography and our prior decisions upholding search warrants despite similar delays, the ten-month delay in obtaining a search warrant for Hampton's residence did not cause the information to be-come stale by the time that [United States Department of Immigration and Customs Enforcement (ICE) Special Agent] Oberholtzer requested the search warrant." [74] Hampton's convictions and sentence were affirmed.

Warrantless Seizure The Supreme Court has consistently held that warrantless seizures are per se unreasonable, with only a few specifically established and well-delineated exceptions. [75] One of those exceptions is exigent circumstances, which require two conditions: "an objectively reasonable basis for concluding that the loss or destruction of evidence is imminent; and that governmental interest being served by the intrusion has been weighed against the individual interest that would be protected if a warrant were required." [76]

In United States v. Bradley, 488 F. App. 99 (6th Cir. July 12, 2012), Eric J. Bradley was convicted and sentenced for receiving visual depictions of minors engaged in sexually explicit conduct, in violation of 18 U.S.C.S. § 2252(a)(2). In his appeal, Bradley contended "that [Fayette County, Kentucky Investigator] Bell had seized his computer without obtaining a search warrant and without Bradley's

consent and that no exception to the warrant requirement applied." [77]

In considering whether the destruction of evidence was imminent in Bradley's case, the panel from the Sixth Circuit stated that "it is objectively reasonable to seize a container an officer has probable cause to believe contains evidence of a crime, rather than leave it unguarded in the hands of a suspect who knows that it will be searched." [78] The panel also considered the balance of interests at stake, stating that "the government's interest in deterring the production and dissemination of child pornography is significant." [79] In ruling that exigent circumstances existed and that the execution of the warrantless seizure was reasonable, the panel affirmed Bradley's conviction and sentence.

Scope of Warrant Under the Fourth Amendment, search war-rants are required to describe with particularity to prevent the seizure of one thing under a warrant describing another, hence providing the scope of the warrant. Appeals based on the scope of the warrant incorporate two is-sues with regard to particularity: whether the warrant supplies adequate information to guide officers in selecting what items to seize, and whether the category of items specified in the warrant is too broad because it includes articles that should not be seized. [80] The requirement for particularity ensures that searches "will not take the character of the wide-ranging exploratory searches the Framers intended to prohibit." [81]

In United States v. Evers, 669 F.3d 645 (6th Cir. Feb. 10, 2012), Ovell Evers, Sr. challenged his conviction and sentence for production of child pornography, in violation of 18 U.S.C.S. § 2251(a); possession of child pornography, in violation of 18 U.S.C.S. § 2252(a)(4)(B); and a forfeiture count under 18 U.S.C.S. § 2253. In his appeal, Evers contended that "although the search warrant authorized the seizure of his computers, camera, and other electronic media, it did not authorize a search of the black computer's hard drive, and the police therefore unlawfully exceeded the scope of the warrant when they searched the contents of the computer with-out obtaining a second warrant." [82] In rendering their decision in this appeal, the panel of judges from the Sixth Circuit noted that although the search warrant used to execute the search of Evers' home was not a model of precision, "it cross-referenced [the investigating officer's] affidavit, which in turn recited the underlying factual circumstances of the alleged sexual crimes, identified the victim, gave the address of Evers' residence, and listed a "Digital Camera, Photo's [sic], Personal Computer and accessories" — items linked by [the victim] to the offenses — as objects subject to seizure." [83] In this instance, the court affirmed both the conviction and sentence for Evers.

Expectation of Privacy The expectation of privacy is derived from Katz v. United States, 389 S. Ct. 347 (Dec. 18, 1967). This Supreme Court ruling deter-mined that intrusion with technology could be classified as a search, and as such could also result in an unreasonable search and seizure if the defendant exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." [84]

In United States v. Wheelock, 772 F.3d 825 (8th Cir. Nov. 20, 2014), Guy Edward Whee-lock appealed his conviction and sentence for receiving child pornography in violation of 18 U.S.C.S. § 2252(a). In this case, Wheelock was arrested after law enforcement used in-formation gleaned from an administrative subpoena to match the defendant to a computer that downloaded child pornography us-ing peer-to-peer software. In his appeal, Wheelock contended that an administrative

subpoena "violated his Fourth Amendment privacy interest in the subscriber information obtained from Comcast." [85] [86]

In deciding his appeal, the panel from the Eighth Circuit determined that the investigating officer requested retrievable information from Comcast, and demonstrated that "that the requested records [were] relevant to an ongoing, legitimate law enforcement investigation of Distribution of Child Pornography." [87] Recognizing that this was all that the current statute required, the court concluded by saying that "federal courts in a federal prosecution do not suppress evidence that is seized by state officers in violation of state law, so long as the search complied with the Fourth Amendment." [88] Based on their decision, the court affirmed Wheelock's conviction and sentence.

4.1.2 Evidence Presented at Trial

Sufficiency of Evidence In United States v. Dixon, 589 F. App. 427 (11th Cir. Oct. 23, 2014), Travis "Rocky" Dixon was convicted of receiving child pornography and possession of child pornography, both in violation of 18 U.S.C.S. § 2252(a) (4) (B). Following his conviction, Dixon contended that the government produced insufficient evidence to prove beyond a reasonable doubt that he was guilty of downloading the child pornography found on a computer in his bedroom.

In reviewing his appeal, the panel for the Eleventh Circuit found that "Dixon's admission that he searched for and downloaded child pornography together with the corroborating evidence of downloaded child pornography found on his computer constituted sufficient evidence for a rational jury to conclude that Dixon knowingly received and possessed child pornography." [89] Dixon's conviction and sentence, in this case, were affirmed. In United States v. Flyer, 633 F.3d 911 (9th Cir. Feb. 8, 2011), Andrew Flyer appealed his conviction "in the U.S. District Court for the District of Arizona under 18 U.S.C.S. § 2252 of attempted transportation and shipping of child pornography, possession of child pornography in violation of 18 U.S.C.S. § 2252(a)(4)(B)." [90]

In his appeal, Flyer argued that "there was insufficient evidence to establish that he exercised dominion and control over the images recovered from the unallocated space on the hard drive. Alternatively, he argues that even if he could be said to have "possessed" the images before their deletion, no evidence indicated that the possession occurred during the time period charged in the indictment." [91]

During its review, the panel from the Ninth Circuit Court of Appeals noted that the government conceded that no evidence was presented that Flyer knew of the presence of the contraband images in the unallocated space on his computer. They also conceded that Flyer did not have the forensic software necessary to view the files in unallocated space. Further, there was no evidence that Flyer ever manipulated the images, and Flyer never admitted to viewing the charged images. The government countered that evidence demonstrating that the charged files were at some point deleted were sufficient to establish possession. The panel from the Ninth Circuit disagreed.

In their opinion, the panel noted that "deletion of an image alone does not support a conviction for knowing possession of child pornography on or about a certain date within the meaning of 18 U.S.C.S. § 2252A. No evidence indicated that on or about April 13, 2004, Flyer could recover or view any of the charged images in unallocated space or that he even knew of their presence there." [92] Consequently, Flyer's conviction for possession of child pornography was reversed. The convictions for attempted shipping of child pornography and possession of child pornography on CDs were affirmed.

Relevancy Digital evidence must be relevant. According to FRE Rule 401, Test for Relevant Evidence, the evidence is relevant if "it has any tendency to make a fact more or less probable than it would be without the evidence; and the fact is of consequence in determining the action." [93] However, relevant evidence may be excluded under Rule 403, Excluding Relevant Evidence for Prejudice, Confusion, Waste of Time or Other Reasons, if "its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." [94]

In United States v. Reynolds, 626 F. App. 610 (6th Cir, 2015), Donald Reynolds appealed his conviction and sentencing for receipt and distribution of child pornography in violation of 18 U.S.C.S. § 2252A(a)(2); and one count of possession of child pornography, in violation of 18 U.S.C.S. § 2252A(a)(5)(B). Reynolds argued that expert witness testimony based on historical cell-site data lacked relevancy and that the district court erred in admitting this evidence.

During a search of his residence on April 7, 2011, agents from the Federal Bureau of Investigation (FBI) discovered over 8,000 images of child pornography on a laptop owned by Reynolds. Reynolds disputed that he had downloaded the images, stating that as many as three other persons living in the house had access to his laptop, including his two adult children. The FBI introduced historical cell-site tracking analysis at trial to assist in their determination of who was not at home during the relevant download periods in their investigation. This information also did not show that Reynolds was absent from the home during the same relevant download periods.

The court determined that the historical cell phone records were relevant because "it was probative as to whether each of four persons who generally had access to a desktop computer was absent from the computer's location while child pornography was downloaded onto that computer." [95] According to the court, the evidence also showed "that Reynolds's absence from the residence could not be demonstrated, permitting an inference that Reynolds was the only one out of four house-hold members who was at the residence during the time child pornography was down-loaded onto a desktop computer in that residence." [96] His conviction and sentence were thusly affirmed by the panel from the Sixth Circuit.

Probative Value In United States v. Ballard, 448 F. App. 987 (11th Cir. Dec. 15, 2011), Kenneth Allen Ballard appealed his conviction for distribution and receipt of child pornography in violation of 18 U.S.C.S. § 2252A(a)(2). Ballard argued that the district court for the Middle District of Alabama had abused its discretion "by allowing into evidence every image and a portion of the videos of child pornography that were charged in the indictment, despite Ballard's stipulation that the 15 pictures and three videos were child pornography." [97] Ballard contended that the images unfairly prejudiced the jury and that the impact of the images off-set its probative value and should have been excluded under Rule 403, Excluding Relevant Evidence.

In considering Ballard's appeal, the court noted that FRE Rule 403 is an "extraordinary remedy which the district court should invoke sparingly and that the balance should be struck in favor of admissibility." [98] In its decision affirming the District Court's ruling, the panel from the Seventh Circuit found that the "relevant evidence of the images and videos was not extrinsic to the crime, but was part of the actual pornography possessed." [99]

Authenticity Digital evidence must be authentic. FRE Rule 901, Authenticating or Identifying Evidence states that to "satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." [100]

To demonstrate the authenticity of digital data being presented as evidence, such as a hard drive from a computer or mobile device, the court must be shown that it "was acquired from a specific computer and/or location, that a complete and accurate copy of digital evidence was acquired, and that it has remained unchanged since it was collected." [101] In practice, this process is called making a forensic image or mirror image, and is well-understood by the courts. "Making a mirror image of the hard drive is central to the examination process and is a routine, technical step taken by well-trained. . . agents. It is done to maintain the integrity and security of the original evidence. A mirror image is an exact duplicate of the entire hard drive and includes all the scattered clusters of the active and deleted files and slack and free space. Having such a mirror image of the hard drive also allows the examiner to reconstruct the steps of the examination at a later time." [102]

A hash value is used to authenticate an individual file within the mirror image of a hard drive, or the forensic image file itself. [103] A hash value is a "unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set . . . 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production." [104]

Case law has further clarified the issue of authenticity. In United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000), the court stated that a "district court has the discretion to determine authenticity, and that determination should not be disturbed on appeal absent a showing that there is no competent evidence in the record to support it." In United States v. Lanzon, 639 F.3d 1293 (11th Cir. May 4, 2011), the court stated that "evidence may be authenticated through the testimony of a witness with knowledge." [106]

Potential evidence is also subject to the FRE Rules 1002 and 1003 for Best Evidence. Rule 1002, Requirement of the Original, states that "[a]n original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise." [107]

With regard to digital evidence, this is best understood in terms of the digital image of the original evidence that is made for analysis purposes. The original is not available, be-cause using it might destroy or alter the original evidence. Rule 1003, Admissibility of Duplicates, allows this type of evidence to be admissible. The rule states that "a duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate." [108]

In United States v. Lebowitz, 676 F.3d 1000 (11th Cir. Apr. 5, 2012), Adam Lebowitz appealed his convictions for producing child pornography in violation of 18 U.S.C.S. § 2251(a), and of attempting to entice a child to engage in unlawful sexual activity in violation of 18 U.S.C.S. § 2422(b). At trial, the United States District Court for the Northern District of Georgia admitted into evidence printed transcripts of chat messages between Lebowitz and a minor whom he was attempting to engage in illegal sexual activity. In his appeal, Lebowitz argued that "admission of the printouts violated the authentication requirement in Federal Rule

of Evidence 901." [109] The minor who produced the printout of the chat sessions in question testified at trial that these printouts accurately represent-ed the conversations he had with Lebowitz, though he could not recall when he had produced the printouts.

In forming its opinion, in this case, the panel relied on previous decisions made by the Eleventh Circuit in finding that "appellate courts reviewing a cold record give particular deference to credibility determinations of a fact-finder who had the opportunity to see live testimony." [110] In so doing, the panel determined that the district court did not err in admitting the chat session printouts into evidence. The conviction and sentence for Lebowitz were therefore affirmed.

Hearsay Under FRE Rule 801, hearsay is an out-of-court statement introduced for the truth of the matter asserted; it applies if the proponent plans to use the record's contents as substantive evidence. [111] Hearsay generally may not be admitted as evidence. With regard to digital evidence, the rules regarding Hearsay apply in two ways: email, text messages, and computer-generated reports are considered written statements, while digital video or audio recordings are considered spoken statements. Regardless, there are specific documents (in written or electronic form) that are considered factual, including computer-generated reports, business records, family records, and public records.

In United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. June 18, 2015), the question before the Ninth Circuit was whether a Google Earth satellite image and a digital tack labeled with GPS coordinates should be considered hearsay.

On January 17, 2003, while near the Mexican border, Paciano Lizarraga-Tirado was arrest-ed as a previously removed alien and charged with illegal re-entry into the United States under 8 U.S.C.S. § 1326. At trial, the defend-ant claimed that he was still on the Mexican side of the border prior to his arrest, awaiting instructions from a smuggler.

The federal agents that arrested Lizarraga-Tirado testified to their familiarity with the border area where they made the arrest and were sure that they arrested him north of the border. The agents recorded the GPS coordinates of the arrest on a hand-held device. A Google Earth satellite image with the GPS coordinates marked was introduced as evidence at trial. By default, Google Earth marks certain areas on an image, such as nearby towns, and bodies of water. The program also offers users two ways to add markers of their own to the maps it produces. First, a user can manually add a tack, or digital marker, to a map, which the user can label. Users can also type GPS coordinates into Google Earth, which then automatically creates a tack at the proper place on the map. Significantly, the map introduced as evidence had the second type of markers produced by Google Earth.

In considering whether the Google Earth image was hearsay, the panel "held that a photograph isn't hearsay because it makes no assertion. Rather, a photograph merely depicts a scene as it existed at a particular time." [112] They determined that the Google Earth program had accurately placed the tack. In their deliberations, the panel produced an ex-act replica of the map introduced at trial, with the GPS coordinates marked exactly as they were in evidence. Further, the user of the program has no role in determining where the marker will be placed on the map because the Google Earth program does that work.

The panel stated that "[b]ecause the program makes the relevant assertion — that the tack is accurately placed at the labeled GPS coordinates — there is no statement as defined by the hearsay rule. In reaching that conclusion, we join other Circuits that

have held that ma-chine statements are not hearsay." The defendant's conviction was subsequently affirmed.

Scientific Merit Since digital evidence produced by computer forensics is considered scientific, it must also meet the Daubert Standard. The standard stems from Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579, 595 (1993), and has five factors for judges to determine whether scientific evidence is admissible in court: testing, peer review, error rate, standards, and acceptance. The Daubert Standard is also applied to expert witnesses in federal criminal trials. Under FRE Rule 702, Opinions and Expert Testimony, the court must determine (a) the ex-pert'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." [115]

In United States v. Stanley, 533 F. App. 325 (4th Cir. July 19, 2013), Paul Stanley appealed his conviction for receipt, transportation, and possession of child pornography in violation of 18 U.S.C.S. § 2252A(a)(1), 18 U.S.C.S. § 2252A(2), and 18 U.S.C.S. § 2252A(a)(5)(B), arguing that the district court erred in admitting expert testimony from an agent who conducted the forensic examination of Stanley's laptop computer. Stanley argued specifically that Agent Crystal Gilmer of the Maryland State Police "possessed in-sufficient specialized knowledge or skill in the software programs used to extract data from Stanley's computer, and failed to offer testimony regarding the reliability of the forensic tools used in the examination." [116]

In examining the pertinent facts, the U.S. Court of Appeals for the Fourth Circuit found that agent Gilmer was part of a lengthy voir dire that established her "education, training, experience, and knowledge of the forensic tools and procedures she utilized, as well as detailed explanations of her use of the forensic software in this particular case." [117] During this proceeding, Agent Gilmer also explained that the tools used to examine the defendant's laptop were accepted as a reliable practice by the Maryland State Police.

In denying Stanley's appeal, the court found that the record strongly supported the determination by the district court of Agent Gil-more's competence as an expert and the reliability of her findings.

4.2 Revisiting the Research Questions

- What was the most common legal basis for appeals of computer forensics evidence? For Search and Seizure related appeals, Probable Cause was the most common basis of an appeal. For Evidence Presented at Trial, the most frequently occurring basis of the appeal was Sufficiency of Evidence.

- How often were cases involving an appeal regarding computer forensics affirmed or reversed for the defense? Of the cases included in this study, twelve appeals (8.16 percent) were affirmed or reversed for the defense.

- What were the most frequently occurring legal grounds for reversed judgments for the defense? Out of the 10 reversals for the defense, five were based on Sufficiency of Evidence.

- What was the most frequently occur-ring legal ground for affirmed judgments for the defense? There were two instances of affirmed judgments for the defense: one

based on a defective warrant and the other based on the scope of the warrant.

- Are some challenges to digital evidence more prevalent than others? If so, why? The majority of challenges seen in this study were based on Search and Seizure issues, rather than the science of computer forensics. The "why" part of the question is more difficult to discern. This study only examined appeals from criminal cases heard by the U.S. Courts of Appeal. Future re-search may involve an in-depth look at cases at the federal district court level to examine this issue.

- Based on the results of this study, are there trends or areas of the law as applied to computer forensics that needs further attention? One area of concern is particularity in regard to the scope of search war-rants. Particularity governs how far the government can search based on a particular factual predicate. Several important cases with regard to particularity have been decided by the courts recently (Riley v. California, 134 S. Ct. 2473 (2014), and United States v. Ganias, 725 F.3d 125 (2d Cir. 2014). This issue will continue to be central to appeals based on Search and Seizure in general, and those involving digital evidence specifically.

5. LIMITATIONS

The overall goal for the current study was to examine the legal basis for appeals related to digital evidence and the subsequent U.S. Circuit Courts of Appeal rulings on such appeals. This study surveyed appeals from federal criminal cases heard before the United States Courts of Appeal from 2010 to 2015. Subsequently, new technologies have become part of the fabric of life, such as storing information in the cloud, or the Internet of Things.

Future research should consider how these newer technologies have affected the legal landscape. For example, future research should investigate the impact of Carpenter v. United States, 138 S. Ct. 2206 (2018) on appeals related to probable cause, or the expectation of privacy. Researchers may want to consider civil matters before the court with regard to digital evidence.

Additionally, the methodology for the current study included analyzing cases from Lexus Nexus. As such, the potential bias of the jurists was outside the scope of the current study. Future researchers may also want to consider any potential bias in the decision making process used by jurists in rendering their opinions.

6. CONCLUSIONS

Of the 145 cases included in this study, only 22 appeals were based on the science of computer forensics, including probative value, authenticity, hearsay, relevancy, and scientific merit. In each of those cases, previous rulings were affirmed. This raises several questions to contemplate:

Overall, digital evidence does not seem to play a large role in federal criminal appeals filed within the U.S. Courts of Appeals. While the search terms used in this study may have missed some of the cases that would otherwise have been included, the fact that only 147 of the 45,030 federal, criminal cases affirmed or reversed for the years 2010 through 2015 raises questions.

- Does digital evidence tend to support previously supported facts of a particular case (i.e., corroborative), or is it so strong as to overbear any evidence to the contrary (i.e., conclusive)?

- What is the frequency with which digital evidence is being admitted in the U.S. District Courts?
- What are the legal bases for those instances where computer forensics is suppressed as evidence?
- Is computer forensics underutilized as evidence?

To answer these questions, it will be necessary to more closely examine the trial proceedings at the U.S. District Court level.

7. NOTES

1. William J. Sabol, "Social Science Research on Forensic Science: Dear Colleague Letter from William Sabol, Fiscal Year 2015," Funding and Awards, last modified December 5, 2014, accessed November 13, 2015, http://nij.gov/funding/pages/fy15-dear-colleague-forensics.aspx.
2. Among others, the following organizations have published "best practices" for computer forensics: National Institute of Standards and Technology (NIST), Federal Bureau of Investigation (FBI), and the National Institute of Justice (NIJ).
3. The State of Georgia v. Justin Ross Harris, Indictment #143124, (Cobb Judicial District, Georgia Oct. 20, 2014).
4. Zachary G. Newman and Anthony Ellis, "The Reliability, Admissibility, and Power of Electronic Evidence," American Bar Association - Section of Litigation, last modified January 25, 2011, https://apps.americanbar.org/litigation/committees/trialevidence/articles/012511-electronic-evidence.html.
5. Matt McCusker, "The Real Danger from Casey Anthony's Trial: Scary Scientific Precedents," Deliberations (blog), entry posted July 4, 2011, accessed November 19, 2015, http://jurylaw.typepad.com/deliberations/2011/07/index.html.
6. Casey Anthony was living at the home of her parents at the time the murder was alleged to have occurred.
7. Craig Wilson, "Digital Evidence Discrepancies – Casey Anthony Trial," Digital Detective, last modified July 11, 2011, accessed November 19, 2015, http://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/.
8. Electronic storage devices include, but not limited to computers, mobile devices, and wearable technology
9. Simson L. Garfinkel, "Digital Forensics," American Scientist 101, no. 5 (September/October 2013), http://www.americanscientist.org/issues/pub/digital-forensics.
10. Ibid
11. Orin S. Kerr, "Search Warrants in an Era of Dig-ital Evidence," Mississippi Law Journal 75, no. 85 (February 11, 2005)
12. Paige Bartholomew, "Seize First, Search Later: The Hunt for Digital Evidence," Touro Law Re-view 30, no. 4 (2014)
13. Thomas K. Clancy, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer," Mississippi Law Journal 75 (2005).
14. 134 S. Ct. 2473 (2014)

Defendant	Circuit	Decided	Legal Issue
Pires; 642 F.3d 1	1	4/6/2011	Sufficiency of Evidence
Crespo-Ríos; 645 F.3d 37	1	6/8/2011	Probable Cause
Salva-Morales; 660 F.3d 72	1	10/31/2011	Sufficiency of Evidence
Kearney; 672 F.3d 81	1	2/29/2012	Defective Warrant
Farlow; 681 F.3d 15	1	6/1/2012	Probable Cause
Chiaradio; 684 F.3d 265	1	7/11/2012	Defective Warrant
Clark; 685 F.3d 72	1	7/16/2012	Probable Cause
Burdulis; 753 F.3d 255	1	5/23/2014	Sufficiency of Evidence
Joubert; 778 F.3d 247	1	2/11/2015	Defective Warrant
Majeroni; 784 F.3d 72	1	4/27/2015	Sufficiency of Evidence
Cordero; 786 F.3d 64	1	5/4/2015	Probable Cause
Burgos-Montes; 786 F.3d 92	1	5/13/2015	Probable Cause
McClellan; 792 F.3d 200	1	7/6/2015	Probable Cause
Figueroa-Lugo; 793 F.3d 179	1	7/17/2015	Sufficiency of Evidence
Broxmeyer; 616 F.3d 120	2	8/3/2010	Sufficiency of Evidence
Rosa; 626 F.3d 56	2	10/27/2010	Defective Warrant
Kornhauser; 519 F. App. 41	2	3/26/2013	Probative Value
Galpin; 720 F.3d 436	2	6/25/2013	Defective Warrant
Sensi; 542 F. App. 8	2	9/20/2013	Probable Cause
Howe; 545 F. App. 64	2	11/24/2013	Probable Cause
Raymonda; 780 F.3d 105	2	3/2/2015	Probable Cause
Vonneida; 601 F. Appx. 38	2	3/2/2015	Sufficiency of Evidence
Bershchansky; 788 F.3d 102	2	6/5/2015	Warrantless Seizure
Thomas; 788 F.3d 345	2	6/11/2015	Probable Cause
Killingbeck; 616 F. Appx. 14	2	10/5/2015	Probable Cause
Konn; 634 F. Appx. 818	2	12/17/2015	Defective Warrant
Miknevich; 638 F.3d 178	3	3/1/2011	Probable Cause

Defendant	Circuit	Decided	Legal Issue
Beatty; 453 Fed. Appx. 204	3	7/14/2011	Probable Cause
Fritz; 453 Fed. Appx. 199	3	11/30/2011	Sufficiency of Evidence
Pavulak; 700 F.3d 651	3	11/21/2012	Probable Cause
Strausbaugh; 534 F. Appx. 178	3	8/9/2013	Probable Cause
Gumbs; 562 F. Appx. 110	3	3/28/2014	Defective Warrant
Epps; 570 F. Appx. 197	3	6/26/2014	Defective Warrant
Husman; 765 F.3d 169	3	9/3/2014	Sufficiency of Evidence
Franz; 772 F.3d 134	3	11/4/2014	Exclusionary Rule
Williams; 592 F.3d 511	4	1/21/2010	Defective Warrant
Bynum; 604 F.3d 161	4	5/5/2010	Expectation of Privacy
Richardson; 607 F. 3d 357	4	6/11/2010	Probable Cause
Rendon; 607 F.3d 982	4	6/17/2010	Expectation of Privacy
Talley; 392 F. Appx. 129	4	8/9/2010	Warrantless Seizure
Hemetek; 393 F. Appx. 67	4	8/26/2010	Probative Value
Russo; 408 F. Appx. 753	4	1/21/2011	Sufficiency of Evidence
Blauvelt; 638 F.3d 281	4	3/9/2011	Probable Cause
Doyle; 650 F.3d 460	4	5/23/2011	Defective Warrant
Wellman; 663 F.3d 224	4	12/7/2011	Defective Warrant
Springstead; 520 Fed. Appx. 168	4	4/15/2013	Scientific Merit
Stanley; 533 F. Appx. 325	4	7/19/2013	Scientific Merit
Myers; 560 F. Appx. 184	4	3/10/2014	Sufficiency of Evidence
Steele; 595 F. Appx. 208	4	12/24/2014	Sufficiency of Evidence
Allen; 625 F.3d 830	5	11/4/2010	Probable Cause
McNealy; 625 F.3d 858	5	11/5/2010	Authenticity
Leet; 406 F. Appx. 830	5	11/19/2010	Sufficiency of Evidence
Oliver; 630 F.3d 397	5	1/6/2011	Probable Cause
Winkler; 639 F.3d 692	5	4/25/2011	Sufficiency of Evidence

Figure 2. APPEALS INCLUDED IN THIS STUDY

15. Harvard Law Review, "Riley v. California," Harvard Law Review, last modified November 10, 2014, accessed April 7, 2017, `http://harvardlawreview.org/2014/11/riley-v-california/`.

16. It is important to note that in Riley, the cell phone was obtained as a result of a search incident to arrest rather than through a search authorized by a warrant. The warrant requirement established in Riley applies to a search of the contents of a cell phone once the cell phone is properly obtained (through an original warrant, search incident to arrest, etc.).

17. Adam M. Gershowitz, "The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches," Vanderbilt Law Review 69, no. 3 (April 2016): 586.

Defendant/Reporter	Circuit	Decided	Legal Issue
Diaz; 435 F. Appx. 329	5	7/29/2011	Warrantless Seizure
Moreland; 665 F.3d 137	5	12/14/2011	Sufficiency of Evidence
Pelland; 494 Fed. Appx. 475	5	10/17/2012	Sufficiency of Evidence
Woerner; 709 F.3d 527	5	2/22/2013	Sufficiency of Evidence
Wyss; 542 F. Appx. 401	5	10/21/2013	Scientific Merit
Larman; 547 F. Appx. 475	5	11/13/2013	Sufficiency of Evidence
Howard; 766 F.3d 414	5	9/9/2014	Sufficiency of Evidence
Roetcisoender; 792 F.3d 547	5	7/2/2015	Sufficiency of Evidence
Oriskawe; 624 F. Appx. 149	5	8/5/2015	Exclusionary Rule
Oufnac; 449 F. Appx. 472	6	12/2/2011	Sufficiency of Evidence
Kernell; 667 F.3d 746	6	1/30/2012	Sufficiency of Evidence
Evers; 669 F.3d 645	6	2/10/2012	Scope of Warrant
Westerlund; 477 F. Appx. 366	6	4/25/2012	Defective Warrant
Bradley; 488 F. Appx. 99	6	7/12/2012	Probable Cause
Hampton; 504 F. Appx. 402	6	11/5/2012	Probable Cause
Kinison; 710 F.3d 678	6	3/19/2013	Probable Cause
Conner; 521 F. Appx. 493	6	4/11/2013	Expectation of Privacy
Rose; 714 F.3d 362	6	4/18/2013	Probable Cause
Fisher; 745 F.3d 200	6	3/7/2014	Exclusionary Rule
Trepanier; 576 F. Appx. 531	6	4/13/2014	Probative Value
Elbe; 774 F.3d 885	6	11/20/2014	Defective Warrant
Pirosko; 787 F. Appx. 358	6	7/16/2015	Scientific Merit
Lowe; 795 F.3d 519	6	7/28/2015	Sufficiency of Evidence
Hentzen; 638 F. Appx. 427	6	8/17/2015	Sufficiency of Evidence
Reynolds; 626 F. Appx. 610	6	9/11/2015	Relevancy
Keith; 440 F. Appx. 503	7	11/4/2011	Probable Cause
Clark; 668 F.3d 934	7	2/13/2012	Probable Cause
Seiver; 692 F.3d 774	7	8/28/2012	Probable Cause
Carroll; 750 F.3d 700	7	4/29/2014	Probable Cause
Harrell; 572 F. Appx. 452	7	7/24/2014	Sufficiency of Evidence
Reichling; 781 F.3d 883	7	3/27/2015	Probable Cause
Koch; 625 F.3d 470	8	11/17/2010	Exclusionary Rule
Darr; 661 F.3d 375	8	11/16/2011	Defective Warrant
Houston; 665 F.3d 991	8	1/11/2012	Probable Cause
Beasley; 688 F.3d 523	8	7/31/2012	Probable Cause
Suing; 712 F.3d 1209	8	4/10/2013	Scope of Warrant
Chase; 717 F.3d 651	8	6/25/2013	Probable Cause
Landsdown; 735 F.3d 805	8	11/7/2013	Sufficiency of Evidence
Manning; 738 F.3d 937	8	1/3/2014	Sufficiency of Evidence
Stringer; 739 F.3d 391	8	1/6/2014	Probable Cause
Robertson; 560 F. Appx. 626	8	3/20/2014	Probative Value
Shellbarger; 770 F.3d 714	8	10/21/2014	Sufficiency of Evidence
Wheelock; 772 F.3d 825	8	11/20/2014	Expectation of Privacy
Evans; 802 F.3d 942	8	9/18/2015	Probative Value
Botta; 405 F. Appx. 196	9	12/8/2010	Defective Warrant
Krupa; 658 F.3d 1174	9	2/7/2011	Probable Cause
Flyer; 633 F.3d 911	9	2/8/2011	Sufficiency of Evidence
Lynn; 636 F.3d 1127	9	5/31/2011	Sufficiency of Evidence
Washington; 661 F.3d 380	9	11/7/2011	Defective Warrant
Budziak; 697 F.3d 1105	9	7/17/2012	Sufficiency of Evidence
Cotterman; 709 U.S. 952	9	3/30/2013	Scope of Warrant
Needham; 718 F.3d 1190	9	6/14/2013	Probable Cause
Johnson; 537 F. Appx. 717	9	8/12/2013	Warrantless Seizure
Sedaghaty; 728 F.3d 885	9	8/23/2013	Scope of Warrant

Figure 3. APPEALS INCLUDED IN THIS STUDY

18. Ibid

19. The good faith exception allows the introduction of evidence that otherwise would have been excluded for violation of privacy rights if law enforcement were acting in good faith when they collected the evidence (i.e., they reasonably thought their actions were lawful).

20. Andrew D. Huynh, "What Comes after 'Get a Warrant': Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley," Cornell Law Review 101, no. 1 (2015): 218.

Defendant/Reporter	Circuit	Decided	Legal Issue
Schesso; 730 F.3d 1040	9	9/18/2013	Probable Cause
Johnston; 789 F.3d 934	9	5/26/2015	Scope of Warrant
Lizarraga-Tirado; 789 F.3d 1107	9	6/18/2015	Hearsay
Henderson; 595 F.3d 1198	10	2/17/2010	Probable Cause
Burkhart; 602 F.3d 1202	10	4/23/2010	Probable Cause
Renigar; 613 F.3d 990	10	7/13/2010	Probable Cause
Burke; 633 F.3d 984	10	2/2/2011	Probable Cause
Easterwood; 415 F. Appx. 883	10	2/23/2011	Probative Value
Benoit; 713 F.3d 1	10	4/2/2013	Warrantless Seizure
Nance; 767 F.3d 1037	10	9/23/2014	Probative Value
Seymour; 598 F. Appx. 867	10	3/27/2015	Relevancy
Krueger; 809 F.3d 1109	10	11/10/2015	Defective Warrant
Edwards; 813 F.3d 953	10	12/29/2015	Probable Cause
South; 359 Fed. Appx. 960	11	1/11/2010	Sufficiency of Evidence
Schwinn; 376 F. Appx. 974	11	4/28/2010	Probable Cause
Vallimont; 378 F. Appx. 972	11	5/11/2010	Warrantless Seizure
Penton; 380 F. Appx. 818	11	5/25/2010	Sufficiency of Evidence
Edens; 380 F. Appx. 880	11	5/26/2010	Sufficiency of Evidence
Vanbrackle; 397 F. Appx. 557	11	9/22/2010	Probable Cause
Pruitt; 638 F.3d 763	11	4/13/2011	Sufficiency of Evidence
Durdley; 436 F. Appx. 966	11	8/9/2011	Scope of Warrant
Barrington; 648 F.3d 1178	11	8/11/2011	Sufficiency of Evidence
Norman; 448 F. Appx. 895	11	11/4/2011	Expectation of Privacy
Ballard; 448 F. Appx. 987	11	12/15/2011	Probative Value
Schaff; 454 F. Appx. 880	11	1/17/2012	Sufficiency of Evidence
Lebowitz; 676 F.3d 1000	11	4/5/2012	Authenticity
Walden; 478 F. Appx. 571	11	5/3/2012	Sufficiency of Evidence
Cowan; U.S. Appx. Lexis 23687	11	11/19/2012	Sufficiency of Evidence
Lovvorn; 524 F. App. 485	11	7/25/2013	Defective Warrant
Curbelo; 726 F.3d 1260	11	8/9/2013	Warrantless Seizure
Bush; 727 F.3d 1308	11	8/27/2013	Probable Cause
Grzybowicz; 747 F.3d 1296	11	4/4/2014	Warrantless Seizure
Ransfer; 749 F.3d 914	11	4/14/2014	Warrantless Seizure
Dixon; 589 F. Appx. 427	11	10/23/2014	Sufficiency of Evidence
Price; 582 F. Appx. 846	11	11/14/2014	Sufficiency of Evidence
Syed; 616 F. Appx. 973	11	9/17/2015	Sufficiency of Evidence
Hester; 627 F. Appx. 867	11	10/1/2015	Hearsay

Figure 4. APPEALS INCLUDED IN THIS STUDY

21. Orin S. Kerr, "Commentary on the Ganias Case," The Washington Post (Washington, DC/USA), June 24, 2014.

22. Ibid

23. Angeli, David H., Christina Schuck, and Avalyn Taylor. "Article: The Plain View Doctrine and Computer Searches: Balancing Law Enforcement's Investigatory Needs with Privacy Rights in the Digital Age." The Champion, Au-gust 2010, 18-24. Accessed April 4, 2017. https://advance.lexis.com/api/permalink/810a0c0a-462b-4302-9f92-4db3c87e81e4/?context=1000516.

24. The plain view doctrine allows a law enforcement officer to seize evidence of a crime, with-out obtaining a search warrant, when that evidence is in plain sight.

25. Hood, Nicholas. "No Requirement Left Behind: The Inadvertent Discovery Requirement—Protecting Citizens One File at a Time." Valparaiso University Law Review 45, no. 4 (Summer 2011): 1529-87.

26. Larry E. Daniel, "Plain View Doctrine in Digital Evidence Cases—a Common Sense Approach," Forensic Magazine, October 23, 2009, http://www.forensicmag.com/

Circuit	Affirmed for Defense	Reversed for Defense	Affirmed for Government	Reversed for Government	Totals
First Circuit	0	1	12	1	14
Second Circuit	1	2	8	1	12
Third Circuit	0	1	8	0	9
Fourth Circuit	0	1	13	0	14
Fifth Circuit	0	1	13	0	14
Sixth Circuit	0	1	14	1	16
Seventh Circuit	0	0	6	0	6
Eighth Circuit	0	0	13	0	13
Ninth Circuit	0	3	8	2	13
Tenth Circuit	1	0	9	0	10
Eleventh Circuit	0	0	24	0	24
Totals	**2**	**10**	**128**	**5**	**145**

Figure 5. SUMMARY TABLES: Summary of Results, By Circuit

Basis of Appeal	Affirmed for Defense	Reversed for Defense	Affirmed for Government	Reversed for Government	Totals
Probable Cause	0	2	35	3	40
Defective Warrant	1	3	14	0	18
Warrantless Seizure	1	0	8	0	9
Scope of Warrant	0	1	4	1	6
Expectation of Privacy	0	0	5	0	5
Exclusionary Rule	0	0	4	0	4
Authenticity	0	0	2	0	2
Relevancy	0	0	2	0	2
Hearsay	0	0	2	0	2
Probative Value	0	0	8	0	8
Scientific Merit	0	0	4	0	4
Sufficiency of Evidence	0	6	39	0	45
Totals	2	12	127	4	145

Figure 6. Summary Results by Legal Issue

article/2009/10/plain-view-doctrine-digital-evidence-cases\%E2\%80\%94-common-sense-approach

27. Jason Weinstein and William Drake, "Public Safety, Privacy, and Particularity: A New Approach to Search Warrants for Digital Evidence," Electronic Commerce & Law Report 19 (May 7, 2014)

28. J. Shane Givens, "The Admissibility of Electronic Evidence at Trial: Courtroom

Defendant	Reporter	Case Number	Circuit	Decided	Basis of Appeal
Cordero-Rosario	786 F.3d 64	14-1007	1	5/4/2015	Probable Cause
Broxmeyer	616 F.3d 120	09-1457	2	8/3/2010	Sufficiency of Evidence
Galpin	720 F.3d 436	11-4808	2	6/25/2013	Probable Cause
Husman	765 F.3d 169	13-2688	3	9/3/2014	Sufficiency of Evidence
Doyle	650 F.3d 460	09-4603	4	5/23/2011	Defective Warrant
Moreland	665 F.3d 137	09-60566	5	12/14/2011	Sufficiency of Evidence
Lowe	795 F.3d 519	14-5615	6	7/28/2015	Sufficiency of Evidence
Flyer	633 F.3d 911	08-10580	9	2/8/2011	Sufficiency of Evidence
Lynn	636 F.3d 1127	09-10242	9	3/31/2011	Sufficiency of Evidence
State of Washington	661 F.3d 380	10-35085	9	11/7/2011	Defective Warrant
Budziak	697 F.3d 1105	11-10223	9	7/17/2012	Sufficiency of Evidence

Figure 7. Summary of Decisions Reversed for the Defense

Defendant	**Reporter**	**Case Number**	**Circuit**	**Decided**	**Basis of Appeal**
Bershchansky	788 F.3d 102	13-3145	2	6/5/2015	Warrantless Seizure
Krueger	809 F.3d 1109	14-3035	10	11/10/2015	Defective Warrant

Figure 8. Summary of Decisions Affirmed for the Defense

Offense	Frequency
Possession of CP	90
Distribution of CP	40
Narcotics	5
Child Exploitation	2
Fraud	2
Obstruction of Justice	1
Production of CP	1
Tax Evasion	1
Theft	1
Murder	1
Weapons Violation	1

Figure 9. Summary of federal offenses

Technology	Frequency
Desktop Computer	98
Laptop	26
External Media	11
Mobile Device	5
GPS Unit	4
Digital Camera	1

Figure 10. Summary of Technologies

Admissibility Standards," Cumberland Law Review 34 (2003).

29. Ibid.

30. Ibid.

31. Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. May 4, 2007).

32. Ibid, 542.

33. Rebecca Levy - Sachs and Taylor Archambault, "Hurdling toward the Future: Navigating Electronically Stored Information through the Federal Rules of Evidence: Lorraine V. Markel America Insurance Co.," 2008 FDCC

Winter Meeting; Technology and E-Commerce/Intellectual Property Section, February 29, 2008, accessed April 4, 2017, http://www.thefederation.org/documents/10.LevySachs.pdf.

34. Jonathan D. Frieden and Leigh M. Murray, "The Admissibility of Electronic Evidence under the Federal Rules of Evidence," Richmond Journal of Law and Technology XVII, no. 2 (2011)

35. Paul D. Grimm, "Authenticating Digital Evidence," GP Solo 31, no. 5 (September/October 2014)

36. Ibid.

37. Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999)

38. Matthew Meyers and Marcus Rogers, "Computer Forensics: The Need for Standardization and Certification," International Journal of Digital Evidence 3, no. 2 (Fall 2004): 5.

39. Ibid, 10.

40. Ibid, 11

41. John S. Atkinson, "Proof Is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System," Birkbeck Law Review 2, no. 2 (December 2014): 253.

42. Simson L. Garfinkel, "Digital Forensics," American Scientist 101, no. 5 (September/October 2013): [Page #], accessed March 14, 2017, http://www.americanscientist.org/issues/pub/digital-forensics.

43. Daniel B. Garrie and J. David Morrissy, "Digital Forensic Evidence in the Courtroom: Under-standing Content and Quality," Northwestern Journal of Technology and Intellectual Property 12, no. 2 (April 2014): 127.

44. James F. Spriggs and Thomas G. Hansford, "Explaining the Overruling of U.S. Supreme Court Precedent," Journal of Politics 63, no. 4 (November 2001): 1107.

45. Sara C. Benesh and Malia Reddick, "Overruled: An Event History Analysis of Lower Court Re-action to Supreme Court Alteration of Precedent," Journal of Politics 64, no. 2 (May 2002): 546.

46. Treatment of precedents may be examined using Shepard's Citations. Established in 1873, it helps legal scholars determine the precedential value of a case through history, evaluates and analyzes what subsequent decisions have said about the precedent, and traces the discussion to specific points of law through the use of head-notes.

47. Benjamin Kassow, Donald R. Songer, and Michael P. Fix, "The Influence of Precedent on State Supreme Courts," Political Research Quarterly 65, no. 2 (March 18, 2011): 380.

48. Richard M. Re, "Narrowing Supreme Court Precedent from Below," Georgetown Law Journal 104, no. 4 (April 2016): 921.

49. Re, "Narrowing Supreme," 921

50. Alan Butler, "Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after Riley v. California," Duke Journal of Constitutional Law & Public Policy 10, no. 1 (October 2014): 21.

51. Ibid, 22.

52. Ibid 24.

53. John S. Atkinson, "Proof Is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System," Birbeck Law Review 2, no. 2 (December 2014)

54. The status of all cases analyzed in this study, confirming whether rulings from that court stood, and whether these rulings received subsequent negative treatment or criticism may found in Appendix I.

55. For the period 2010 – 2015, there were 45.030 criminal appeals where the outcome was either affirmed or re-versed for all United States Circuit Courts of Appeals (92.2 percent were affirmed for the government, while 7.8 percent were reversed for the defendant).

56. Thomas K. Clancy, "Digital Child Pornography and the Fourth Amendment," Judges' Journal 49, no. 3 (Summer 2010): 26.

57. Federal Rules of Evidence, 28 U.S.C. §§ 93-595 (1975 & Supp. 2014).

58. Weeks v. United States, 232 U.S. 383 (1914)

59. "Olmstead v. United States: The Constitutional Challenges of Prohibition Enforcement — Historical Background and Documents," History of the Federal Judiciary, last modified 2016, ac-cessed August 10, 2016, `http://www.fjc.gov/history/home.nsf/page/tu_olmstead_questions.html`.

60. United States v. Watson, 423 U.S. 411 (1976)

61. See Weeks v. United States, 232 U.S. 383, 392 (1914); Carroll v. United States, 267 U.S. 132, 158 (1925); Agnello v. United States, 269 U.S. 20, 30 (1925)

62. See Carroll v. United States, 267 U.S. 132, 158 (1925); Chambers v. Maroney, 399 U.S. 42 (1970); Arizona v. Johnson, 129 S. Ct. 781, 786 (2009); Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990); United States v. Martinez-Fuerte, 428 U.S. 543 (1976);and City of Indianapolis v. Edmond, 531 U.S. 32 (2000)

63. See 265 U.S. 57 (1924), 466 U.S. 170 (1984), and California v. Greenwood, 486 U.S. 35 (1988)

64. See Steele v. United States, 267 U.S. 498 (1925); Arizona v. Hicks, 480 U.S. 321 (1987); and Illinois v. Andreas, 463 U.S. 765, 771 (1983).

65. See New Jersey v. T.L.O, 469 U.S. 325 (1985); and Safford Unified School District #1 v. Red-ding, 129 S. Ct. 2633 (2009).

66. See Hudson v. Palmer, 468 U.S. 517, 526 (1984) for prison cell searches; and Griffin v. Wisconsin, 483 U.S. 868 (1987) for probation.

67. See Skinner v. Railway Labor Executives' Ass'n4, 89 U.S. 602 (1989); and upheld in National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989)

68. United States v. Schesso, 730 F.3d 1040, (9th Cir. 2013).

69. Ibid.

70. United States v. Frechette, 583 F.3d 374 (6th Cir. Oct. 8, 2009)

71. Ibid.

72. United States v. Terry, 522 F.3d 645, 650 n.2 (6th Cir. 2008).

73. United States v. Hampton, 504 F. App. 402 (6th Cir. Nov. 5, 2012)

74. Ibid.

75. See United States v. Jacobsen, 466 U.S. 109, and United States v. Matlock, 415 U.S. 164.

76. United States v. Plavcak, 411 F.3d 655 (6th Cir. June 6, 2005)

77. United States v. Bradley, 488 F. App. 99, (6th Cir. July 12, 2012)

78. Ibid.

79. Ibid. Citing United States v. Moore, 916 F.2d 1131, 1139 (6th Cir. 1990)

80. United States v. Richards, 659 F.3d 527 (6th Cir. Tenn. 2011)

81. Marron v. United States, 275 U.S. 192, 196 (1927)

82. United States v. Evers, 669 F.3d 645 (6th Cir. Feb. 10, 2012)

83. Ibid.

84. Katz v. United States, 389 U.S. 347 (U.S. Dec. 18, 1967).

85. United States v. Wheelock, 772 F.3d 825 (8th Cir. Nov. 20, 2014)

86. An administrative subpoena under U.S. law is issued by a federal agency without prior judicial oversight.

87. United State v. Wheelock.

88. Ibid. Citing United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002).

89. United States v. Dixon, 589 F. App. 427 (11th Cir. Oct. 23, 2014).

90. United States v. Flyer, 633 F.3d 911, (9th Cir. Feb. 8, 2011)

91. Ibid.

92. United States vs. Flyer 2011.

93. Cornell Law School, "Rule 401. Test for Rele-vant Evidence," Legal Information Institute, last modified 2015, accessed November 13, 2015, https://www.law.cornell.edu/rules/fre/rule_401.

94. Cornell Law School, "Rule 403. Excluding Rel-evant Evidence for Prejudice, Confusion, Waste of Time, or Other Reasons," Legal Information Institute, last modified 2015, accessed Novem-ber 13, 2015, https://www.law.cornell.edu/rules/fre/rule_403.

95. United States v. Reynolds, 626 F. App. 610 (6th Cir, 2015)

96. 626 F. App. 610

97. United States v. Ballard, 448 F. App. 987

98. Ibid, quoting United States v. Dodds, 347 F.3d 893 (2003)

99. Ibid

100. Cornell Law School, "Rule 901. Authenticating or Identifying Evidence," Legal Information In-stitute, last modified 2015, accessed November 19, 2015, https://www.law.cornell.edu/rules/fre/rule_901.

101. Eoghan Casey, "Digital Evidence in the Court-room," in Digital Evidence and Computer Crime, 3rd ed. (New York, NY: Elsevier, 2011), 60.

102. United States v. Crim. Triumph Capital Group, 211 F.R.D. 31 (D. Conn. 2002)

103. For a discussion on forensic image file formats, see Forensics File Formats, Forensics Wiki, http://www.forensicswiki.org/wiki/Category:Forensics_File_Formats.

104. Barbara J. Rothstein, Ronald J. Hedges, and Elizabeth C. Wiggins, "Managing Discovery of Electronic Information: A Pocket Guide for Judges," Federal Evidence Review, last modi-fied 2007, accessed March 27, 2017, http://federalevidence.com/pdf/2008/09-Sept/FJC_\%20Managing\%20Discovery\%20of\%20Electronic\%20Information.pdf.

105. United States v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000)

106. United States v. Lanzon, 639 F.3d 1293 (11th Cir. May 4, 2011)

107. Cornell Law School, "Rule 1002. Requirement of the Original," Legal Information Institute, last modified 2015, accessed November 19, 2015, https://www.law.cornell.edu/rules/fre/rule_1002

108. Cornell Law School, "Rule 1003. Admissibility of Duplicates," Legal Information Institute, last modified 2015, accessed November 19, 2015, https://www.law.cornell.edu/rules/fre/rule_1003.

109. 109. United States v. Lebowitz, 676 F.3d 1000 (11th Cir. Apr. 5, 2012)

110. 110. Owens v. Wainwright, 698 F.2d 1111, 1113 (11th Cir. 1983)

111. Cornell Law School, "Rule 801. Exclusions from Hearsay," Legal Information Institute, last modified 2015, accessed November 13, 2015, https://www.law.cornell.edu/rules/fre/rule_801.

112. United States v. Lizarraga-Tirado, 789 F.3d 1107. Also, see United States v. May, 622 F.2d 1000, 1007 (9th Cir. 1980); wherein Apprehen-sion Data Cards were not hearsay because they were not "offered in evidence to prove the truth of the matter asserted. The photographs on them were introduced as circumstantial evidence."

113. Ibid

114. Kumho Tire Co. v. Carmichael, 524 U.S. 936 (U.S. 1998) extended Daubert to include any form of technical evidence.

115. Cornell Law School, "Rule 702. Testimony by Expert Witnesses," Legal Information Institute, last modified 2015, accessed November 13, 2015, https://www.law.cornell.edu/rules/fre/rule_702.

116. United States v. Stanley, 533 F. App. 325, (4th Cir. July 19, 2013)

117. Ibid.

118. No subsequent action includes those cases where US Supreme Court certiorari was denied

119. Validity questioned in United States v. Wencewicz, 63 F. Supp. 3d 1238, 2014 U.S. Dist. LEXIS 151322 (D. Mont. Oct. 24, 2014)

120. Criticized in United States v. Unknown (In re Unknown), 701 F.3d 749, 2012 U.S. App. LEX-IS 23802 (5th Cir. Tex. Nov. 19, 2012)

121. United States v. Graves, 951 F. Supp. 2d 758, 2013 U.S. Dist. LEXIS 90324 (E.D. Pa. June 27, 2013)

122. United States v. Unknown (In re Unknown), 701 F.3d 749, 2012 U.S. App.

LEXIS 23802 (5th Cir. Tex. Nov. 19, 2012)

123. United States v. Adams, 2016 U.S. Dist. LEXIS 105471 (M.D. Fla. Aug. 10, 2016)

REFERENCES

[1] [Special issue]. (2015). Cornell Law Review, 101(1).

[2] Administrative Office of the U.S. Courts, Cases Filed, Terminated, and Pending (Summary), Doc. No. Table 2 (). Retrieved from http://www.uscourts.gov/file/19017/download

[3] AmiNarh, J. T., & Williams, P. A.H. (2008). Digital forensics and the legal system: A dilemma of our times. Australian digital forensics conference.

[4] Angeli, D. H., Schuck, C., & Taylor, A. (2010, August). Article: The plain view doctrine and computer searches: Balancing law enforce-ment's investigatory needs with privacy rights in the digital age. The Champion, 18-24. Retrieved from https://advance.lexis.com/api/permalink/810a0c0a-462b-4302-9f92-4db3c87e81e4/?context=1000516

[5] Arizona v. Hicks, 480 S. Ct. 321 (1987).

[6] Atkinson, J. S. (2014). Proof is not binary: The pace and complexity of computer systems and the challenges digital evidence poses to the legal system. Birkbeck Law Review, 2(2), 245-261.

[7] Bagley, W. A. (2011). Don't be evil: The fourth amendment in the age of google, national security, and digital papers and effects. Albany Law Journal of Science Technology, 21(1), 153-192.

[8] Barbara, J. J. (2012, September 4). Computer forensics standards and controls. Forensic Magazine. Retrieved from https://www.forensicmag.com/article/2012/09/computer-forensics-standards-and-controls.

[9] Bartholomew, P. (2014). Seize first, search later: The hunt for digital evidence. Touro Law Re-view, 30(4), 10.

[10] Benesh, S. C., & Reddick, M. (2002). Overruled: An event history analysis of lower court reaction to Supreme Court alteration of precedent. Journal of Politics, 64(2), 534-550.

[11] Butler, A. (2014). Get a warrant: The Supreme Court's new course for digital privacy rights after riley v. California. Duke Journal of Constitutional Law & Public Policy, 10(1), 83-108.

[12] Casey, E. (2011). Digital evidence in the court-room. In Digital evidence and computer crime (3rd ed., pp. 49-82). New York, NY: Elsevier.

[13] Chism v. State of Washington, 661 F.3d 380 (9th Cir. Nov. 7, 2011).

[14] Churchill, M. H., Mauler, D. D., McLaughlin, M. J., & Vincent, M. K. (2015). Admitting and authenticating electronic evidence in court, including trial-like demonstrations. The federal bar association's 2015 federal litigation conference, pp. 1-20.

[15] Churchill, M. H., Mauler, D. D., McLaughlin, M. J., & Vincent, M. K. (2015, October 27). Admitting and authenticating electronic evidence in court, including trial-like demonstrations. Paper presented at The Federal Bar Association's 2015 Federal Litigation Conference, Salt Lake City, Utah/USA.

[16] Clancy, T. K. (2005). The fourth amendment aspects of computer searches and seizures: A perspective and a primer. Mississippi Law Journal, 75, 193-272.

[17] Clancy, T. K. (2010). Digital child pornography and the fourth amendment. Judges' Journal, 49(3), 26-32.

[18] Clark, W. (2015). Protecting the privacies of digital life: Riley v. California, the fourth amendment's particularity requirement, and search protocols for cell phone search warrants. Bos-ton College Law Review, 56(5), 1981-2018.

[19] Cole, K. A., Gupta, S., Gurugubelli, D., & Rogers, M. K. (2015). A review of recent case law related to digital forensics: The current issues. 2015 ADFSL conference on digital forensics, security and law, pp. 95-104.

[20] Congressional Research Agency Library of Congress. (1996). The constitution of the United States of America: Analysis and interpretation (Report No. 103–6) (J. H. Killian & G. A. Costello, Eds.). Washington, DC/USA: U.S. Government Printing Office.

[21] Court role and structure. (n.d.). Retrieved February 7, 2017, from United States Courts web-site: http://www.uscourts.gov/about-federal-courts/court-role-and-structure.

[22] Crocker, A. (2016, June 3). Appeals court avoids hard questions about the "Collect it all" approach to computer searches [Blog post]. Retrieved from DeepLinks Blog: https://www.eff.org/deeplinks/2016/06/appeals-court-avoids-hard-questions-about-collect-it-all-approach-computer.

[23] Daniel, L. E. (2009, October 23). Plain view doctrine in digital evidence cases—a common sense approach. Forensic Magazine. Retrieved from http://www.forensicmag.com/article/2009/10/plain-view-doctrine-digital-evidence-cases\%E2\%80\%94-common-sense-approach.

[24] Digital duplications and the fourth amendment. (2016). Harvard Law Review, 129(4), 1046. Editorial Board. (2014). Riley v. California. Harvard Law Review, 128(1). Retrieved from http://harvardlawreview.org/2014/11/riley-v-california/.

[25] Epstein, J. (2016). Child pornography and exploitation. In A. Morosco (Comp.), The prosecution and defense of sex crimes (Rev. ed.). Retrieved from https://www.lexis.com/research/retrieve?_m=9cc0553738975770940ffffafb78ac5a&csvc=toc2doc&cform=&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVzk-zSkAl&_md5=685308ea17f6414e6a924c278fe5dec1.

[26] Expectation of privacy. (2009, September 17). Retrieved December 20, 2016, from Legal In-formation Institute web-site: https://www.law.cornell.edu/wex/expectation_of_privacy.

[27] Febus, C., Claude, J., & Singer, K. (2010, Febru-ary). Understanding probable cause and over-coming staleness issues in child pornography cases. CEOS Quarterly Newsletter, 9-20.

[28] Federal Rules of Evidence, 28 U.S.C. §§ 93-595 (1975 & Supp. 2014).

[29] Frieden, J. D., & Murray, L. M. (2011). The admissibility of electronic evidence

under the federal rules of evidence. Richmond Journal of Law and Technology, XVII (2).

[30] Friess, N. (2013). When rummaging goes digital: Fourth amendment particularity and stored e-mail surveillance. Nebraska Law Journal, 90(4), 972-1016.

[31] Frost, A. (2015). Inferiority complex: Should state courts follow lower federal court precedent on the meaning of federal law? Vanderbilt Law Review, 68, 53-103.

[32] Galves, F., & Galves, C. (2004). Ensuring the admissibility of electronic forensic evidence and enhancing its probative value at trial. Criminal Justice Magazine, 19(1).

[33] Garfinkel, S. L. (2010). Digital forensics re-search: The next 10 years. Digital Investiga-tion, 7(Supplemental), S64-S73. Garfinkel, S. L. (2013). Digital forensics. Ameri-can Scientist, 101(5), 370. Retrieved from http://www.americanscientist.org/issues/pub/digital-forensics.

[34] Garrie, D. B., & Morrissy, J. D. (2014). Digital forensic evidence in the courtroom: Under-standing content and quality. Northwestern Journal of Technology and Intellectual Prop-erty, 12(2), 121-128.

[35] Gershowitz, A. M. (2016). The postriley search warrant: Search protocols and particularity in cell phone searches. Vanderbilt Law Review, 69(3), 585-638.

[36] Givens, J. S. (2003). The admissibility of electronic evidence at trial: Courtroom admissibility standards. Cumberland Law Review, 34, 95.

[37] Goldfoot, J. (2011). The physical computer and the fourth amendment, Berkeley Journal of Criminal Law, 16(1), 112. Retrieved from http://scholarship.law.berkeley.edu/bjcl/vol16/iss1/3.

[38] Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system (Research Report No. RR-890-NIJ). Santa Monica, CA: RAND. Grimm, P. D. (2014). Authenticating digital evidence. GP Solo, 31(5), 47-49.

[39] Grimm, P. W., & Brady, K. F. (n.d.). Admissibility of electronic evidence [Blog post]. Retrieved from Drug Device Law Blog: https://www.reedsmith.com/files/uploads/DrugDeviceLawBlog/Electronic_Evidence_-_Admission_Guide_pdf.pdf#page=1&zoom=auto,-35,798.

[40] Gruenspecht, J. (2011). "Reasonable" grand jury subpoenas: Asking for information in the age of big data. Harvard Journal of Law & Technology, 24(543).

[41] Hart, A. (2014, July 26). In court, digital evidence can shine or fizzle. The Atlanta Journal-Constitution. Retrieved from http://www.myajc.com/news/crime--law/court-digital-evidence-can-shine-fizzle/dsdyFH23L3IZZaoTrLYZAO/.

[42] Holley, B. (2010). Digitizing the fourth amendment: Limiting the private search exception in computer investigations. Virginia Law Re-view, 96(3), 677-717.

[43] Hood, N. (2011). No requirement left behind: The inadvertent discovery requirement—protecting citizens one file

at a time. Valparai-so University Law Review, 45(4), 1529-1587. How courts work. (2016). Retrieved January 15, 2016, from American Bar Association - Division for Public Education website: http://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/appeals.html.

[44] Huynh, A. D. (2015). What comes after "get a warrant": Balancing particularity and practicality in mobile device search warrants post-Riley. Cornell Law Review, 101(1), 187-222.

[45] Jekot, W. (2007). Computer forensics, search strategies, and the particularity requirement. University of Pittsburgh School of Law Journal of Technology Law and Policy, 7, 1-44.

[46] The Judiciary Act of 1789, 1 Stat. 73 U.S.C. § SEC. 35 (1789).

[47] Kassow, B., Songer, D. R., & Fix, M. P. (2011). The influence of precedent on state supreme courts. Political Research Quarterly, 65(2), 372-384.

[48] Katz v. United States, 389 S. Ct. 347 (Dec. 18, 1967). Kerr, O. S. (2003). A user's guide to the stored communications act, and a legislator's guide to amending it. George Washington Law Re-view, 72, 1208-1243.

[49] Kerr, O. S. (2005). Searches and seizures in a dig-ital world. Harvard Law Review, 119(2), 531-585.

[50] Kerr, O. S. (2005). Search warrants in an era of digital evidence. Mississippi Law Journal, 75(85).

[51] Kerr, O. S. (2010). Fourth amendment seizures of computer data. Yale Law Journal, 119(4), 700-724.

[52] Kerr, O. S. (2011, June 23). The historical role of warrants, particularity, and magistrates [Blog post]. Retrieved from The Volokh Conspiracy website: http://volokh.com/2011/06/23/the-historical-role-of-warrants-particularity-and-magistrates/.

[53] Kerr, O. S. (2013). Foreword: Accounting for technological change. Harvard Journal of Law and Public Policy, 36, 403-408.

[54] Kerr, O. S. (2014, June 24). Commentary on the Ganias case. The Washington Post.

[55] Kerr, O. S. (2015). Executing warrants for digital evidence: The case for use restrictions on non-responsive data. Texas Tech Law Review, 48(1), 1-36.

[56] Knapp, M. (2015, July 6). Second circuit grants rehearing in United States V. Ganias [Blog post]. Retrieved from Lawfare website: https://www.lawfareblog.com/second-circuit-grants-rehearing-united-states-v-ganias#.

[57] Kozel, R. J. (2014). The scope of precedent. Michigan Law Review, 113(1), 179-230.

[58] Kumho Tire Co. v. Carmichael, 119 U.S. 1167 (Mar. 23, 1999). Lee county man nets 17 1/2 years in federal prison for downloading child pornography on LimeWire. (2011, January 12). Retrieved March 17, 2017, from The U.S. Attorney's Office for the Middle District of Alabama website: https://www.justice.gov/archive/usao/alm/press/2011/2011_01_12_ballard.html.

[59] Levy - Sachs, R., & Archambault, T. (2008). Hurdling toward the future: Navigating elec-tronically stored information through the federal rules of evidence: Lorraine V. Markel America Insurance co. 2008 FDCC winter meeting; Technology and e-commerce/intellectual property section, pp. 6-13. Retrieved from http://www.thefederation.org/documents/10.LevySachs.pdf.

[60] Liles, S., Rogers, M., & Hoebich, M. (2009). [A Survey of the Legal Issues Facing Digital Forensic Experts]. In G. Peterson & S. Shenoi (Eds.), Advances in digital forensics V (Vol. 306, pp. 266-267). Berlin, Germany: Springer.

[61] Mantei, C. J. (2011). Pornography and privacy in plain view: Applying the plain view doctrine to computer searches. Arizona Law Review, 53(3), 985-1012. Retrieved from http://arizonalawreview.org/mantei/.

[62] Mestitz, M. (2017). Unpacking digital containers: Extending Riley's reasoning to digital files and subfolders. Stanford Law Review, 69(1), 321-357.

[63] Meyer, D. L. (2009). MelendezDiaz v. Massachusetts: What the expanded confrontation clause ruling means for computer forensics and electronic discovery. Temple Journal of Science, Technology & Environmental Law, 28(2), 243.

[64] Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. International Journal of Digital Evidence, 3(2). Meyers, M., & Rogers, M. (2005). Digital forensics: Meeting the challenges of scientific evidence. In S. Shenoi & M. Pollitt (Eds.), Advances in digital forensics (pp. 43-50). New York, NY: International Federation for Information Processing.

[65] Meyers, M., & Rogers, M. (2006, fall). Computer forensics: The need for standardization and certification. In M. Pollitt & S. Shenoi (Eds.), Advances in digital forensics (Vol. 194, pp. 42-50). New York, NY: Springer International Publishing.

[66] Miranda v. Arizona, 384 U.S. 486 (June 13, 1966).

[67] Murphy, E. (2014). The mismatch between twenty-first-century forensic evidence and our antiquated criminal justice system. Southern California Law Review, 87(3), 633-672.

[68] Nance, K., & Ryan, D. J. (2011). Legal aspects of digital forensics: A research agenda. Proceedings of the 44th Hawaii international conference on system sciences (HICSS-44), pp. 1-6. Newman, Z. G., & Ellis, A. (2011, January 25). The reliability, admissibility, and power of electronic evidence. Retrieved from American Bar Association - Section of Litigation website: https://apps.americanbar.org/litigation/committees/trialevidence/articles/012511-electronic-evidence.html.

[69] Newman, Z. G., & Ellis, A. (2011, January 25). The reliability, admissibility, and power of electronic evidence. Retrieved March 15, 2017, from Section of Litigation Trial Evidence website: https://apps.americanbar.org/litigation/committees/trialevidence/articles/012511-electronic-evidence.html.

[70] Ohm, P. (2005). The fourth amendment right to delete. Harvard Law Review Forum, 119, 10-18. Ohm, P. (2011). Massive hard drives, general warrants, and the power of magistrate judges. Virginia Law Review, 97, 1-12.

[71] Olmstead v. United States: The constitutional challenges of prohibition enforcement — historical background and documents. (2016). Retrieved August 10, 2016, from History of the Federal Judiciary website: http://www.fjc.gov/history/home.nsf/page/tu_olmstead_questions.html.

[72] Re, R. M. (2016). Narrowing Supreme Court precedent from below. Georgetown Law Journal, 104(4), 921-971.

[73] Riley v. California, 134 S. Ct. 2473 (2014).

[74] Riley v. California. (2014). Harvard Law Review, 128(1). Retrieved from http://harvardlawreview.org/2014/11/riley-v-california/.

[75] Rothstein, B. J., Hedges, R. J., & Wiggins, E. C. (2007). Managing discovery of electronic in-formation: A pocket guide for judges. Retrieved March 27, 2017, from Federal Evi-dence Review website: http://federalevidence.com/pdf/2008/09-Sept/FJC_\%20Managing\%20Discovery\%20of\%20Electronic\%20Information.pdf.

[76] Rule 801. Exclusions from hearsay. (2015). Retrieved November 13, 2015, from Legal In-formation Institute website: https://www.law.cornell.edu/rules/fre/rule_801.

[77] Rule 401. Test for relevant evidence. (2015). Retrieved November 13, 2015, from Legal In-formation Institute website: https://www.law.cornell.edu/rules/fre/rule_401.

[78] Rule 403. Excluding relevant evidence for preju-dice, confusion, waste of time, or other rea-sons. (2015). Retrieved November 13, 2015, from Legal Information Institute website: https://www.law.cornell.edu/rules/fre/rule_403.

[79] Rule 901. Authenticating or identifying evidence. (2015). Retrieved November 19, 2015, from Legal Information Institute website: https://www.law.cornell.edu/rules/fre/rule_901.

[80] Rule 1003. Admissibility of duplicates. (2015). Retrieved November 19, 2015, from Legal In-formation Institute website: https://www.law.cornell.edu/rules/fre/rule_1003.

[81] Rule 1002. Requirement of the original. (2015). Retrieved November 19, 2015, from Legal In-formation Institute website: https://www.law.cornell.edu/rules/fre/rule_1002.

[82] Rule 702. Testimony by expert witnesses. (2015). Retrieved November 13, 2015, from Legal In-formation Institute website: https://www.law.cornell.edu/rules/fre/rule_702.

[83] Rummel, J. A. (2011). When warrants uncover digital evidence: The tenth circuit's ruling in United States V. burke. Oklahoma City University Law Review, 36(3), 713-735.

[84] Ryan, D. J., & Shpantzer, G. (2002). Legal aspects of digital forensics. Proceedings: Foren-sics workshop.

[85] Salgado, R. P. (2013). Fourth amendment search and the power of the hash.

Federal Evidence Review. Retrieved from http://federalevidence.com/pdf/2013/02Feb/EE-4thAmSearch-Power\%20of\%20Hash.pdf.

[86] Spriggs, J. F., & Hansford, T. G. (2001). Explaining the overruling of U.S. Supreme Court precedent. Journal of Politics, 63(4), 1091-1111. Statistical tables for the federal judiciary. (n.d.). Retrieved January 13, 2016, from United States Courts website: http://www.uscourts.gov/statistics-reports/analysis-reports/statistical-tables-federal-judiciary.

[87] Statistical tables for the federal judiciary - December 2015. (2015, December 31). Retrieved January 17, 2017, from United States Courts website: http://www.uscourts.gov/statistics-reports/statistical-tables-federal-judiciary-december-2015.

[88] Statistics & reports. (2015, December). Retrieved December 9, 2015, from United States Courts website: http://www.uscourts.gov/statistics-reports. SWGDE digital & multimedia evidence glossary (Report No. Version 3.0). (n.d.). Retrieved from https://www.swgde.org/documents/Current\%20Documents/SWGDE\%20Digital\%20and\%20Multimedia\%20Evidence\%20Glossary.

[89] Thomson, L. L. (2013). Mobile devices: New challenges for admissibility of electronic evidence. The SciTech Lawyer, 9(3&4). United States Code, 2006 Edition, Supplement 5, Title 18 - CRIMES AND CRIMINAL PRO-CEDURE, 18 U.S.C. § 110 (2006 & Supp. 2011).

[90] United States v. Allen, 625 F.3d 830 (5th Cir. Nov. 4, 2010).

[91] United States v. Ballard, 448 F. App. 987 (11th Cir. Dec. 15, 2011).

[92] United States v. Barrington, 648 F.3d 1178 (11th Cir. Aug. 11, 2011).

[93] United States v. Beasley, 688 F.3d 523 (8th Cir. July 31, 2012).

[94] United States v. Beatty, 437 F. App. 185 (3d Cir. July 14, 2011).

[95] United States v. Benoit, 713 F.3d 1 (10th Cir. Apr. 2, 2013).

[96] United States v. Bershchansky, 788 F.3d 102 (2d Cir. June 5, 2015).

[97] United States v. Blauvelt, 638 F.3d 281 (4th Cir. Mar. 9, 2011). 09-4601

[98] United States v. Botta, 405 F. App. 196 (9th Cir. Dec. 8, 2010).

[99] United States v. Bradley, 488 F. App. 99 (6th Cir. July 12, 2012).

[100] United States v. Broxmeyer, 616 F.3d 120 (2d Cir. Aug. 3, 2010).

[101] United States v. Budziak, 697 F.3d 1105 (9th Cir. July 17, 2012).

[102] United States v. Burdulis, 753 F.3d 255 (1st Cir. May 23, 2014).

[103] United States v. Burgos, 786 F.3d 92 (1st Cir. May 13, 2015).

[104] United States v. Burke, 633 F.3d 984 (10th Cir. Feb. 2, 2011).

[105] United States v. Burkhart, 602 F.3d 1202 (10th Cir. Apr. 23, 2010).

[106] United States v. Bush, 727 F.3d 1308 (11th Cir. Aug. 27, 2013).

[107] United States v. Bynum, 604 F.3d 161 (4th Cir. May 5, 2010).

[108] United States v. Carroll, 750 F.3d 700 (7th Cir. Apr. 29, 2014).

[109] United States v. Chase, 717 F.3d 651 (8th Cir. June 25, 2013).

[110] United States v. Chiaradio, 684 F.3d 265 (1st Cir. July 11, 2012).

[111] United States v. Clark, 668 F.3d 934 (7th Cir. Feb. 13, 2012).

[112] United States v. Clark, 685 F.3d 72 (1st Cir. July 16, 2012).

[113] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. Aug. 26, 2009).

[114] United States v. Connor, 521 F. App. 493 (6th Cir. Apr. 11, 2013).

[115] United States v. Cordero-Rosario, 786 F.3d 64 (1st Cir. May 4, 2015).

[116] United States v. Cotterman, 709 U.S. 952 (9th Cir. Mar. 30, 2013).

[117] United States v. Cowan, No. 11-15989 (11th Cir. Nov. 19, 2012).

[118] United States v. Crespo, 645 F.3d 37 (1st Cir. June 8, 2011).

[119] United States v. Crespo-Rios, 645 F.3d 37 (1st Cir. June 8, 2011).

[120] United States v. Curbelo, 726 F.3d 1260 (11th Cir. Aug. 9, 2013).

[121] United States v. Darr, 661 F.3d 375 (8th Cir. Nov. 16, 2011).

[122] United States v. Dawson, 425 F.3d 389 (7th Cir. 2005).

[123] United States v. Diaz, 435 F. App. 329 (5th Cir. July 29, 2011).

[124] United States v. Dixon, 589 F. App. 427 (11th Cir. Oct. 23, 2014).

[125] United States v. Doyle, 650 F.3d 460 (4th Cir. May 23, 2011).

[126] United States v. Dudley, 804 F.3d 506 (1st Cir. Oct. 30, 2015).

[127] United States v. Durdley, 436 F. App. 966 (11th Cir. Aug. 9, 2011).

[128] United States v. Easterwood, 415 F. App. 883 (10th Cir. Feb. 23, 2011).

[129] United States v. Edens, 380 F. App. 880 (11th Cir. May 26, 2010).

[130] United States v. Edwards, 813 F.3d 953 (10th Cir. Dec. 29, 2015).

[131] United States v. Elbe, 774 F.3d 885 (6th Cir. Nov. 20, 2014).

[132] United States v. Epps, 570 F. App. 197 (3d Cir. June 26, 2014).

[133] United States v. Evans, 802 F.3d 942 (8th Cir. Sept. 18, 2015).

[134] United States v. Evers, 669 F.3d 645 (6th Cir. Feb. 10, 2012).

[135] United States v. Farlow, 681 F.3d 15 (1st Cir. June 1, 2012).

[136] United States v. Figueroa, 793 F.3d 179 (1st Cir. July 17, 2015).

[137] United States v. Fisher, 745 F.3d 200 (6th Cir. Mar. 7, 2014).

[138] United States v. Flyer, 633 F.3d 911 (9th Cir. Feb. 8, 2011).

[139] United States v. Franz, 772 F.3d 134 (3d Cir. Nov. 4, 2014).

[140] United States v. Frechette, 583 F.3d 374 (6th Cir. Oct. 8, 2009).

[141] United States v. Fritz, 453 F. App. 204 (3d Cir. Nov. 30, 2011).

[142] United States v. Galpin, 720 F.3d 436 (1st Cir. June 25, 2013).

[143] United States v. Ganias, 725 F.3d 125 (2d Cir. 2014).

[144] United States v. Ganias, 2016 F. App. 9706 (2d Cir. 2016).

[145] United States v. Ganias - second circuit creates a potential "right to deletion" of imaged hard drives. (2014). Harvard Law Review, 128(743). Retrieved from http://harvardlawreview.org/2014/12/united-states-v-ganias/.

[146] United States v. Grzybowicz, 747 F.3d 1296 (11th Cir. Apr. 4, 2014).

[147] United States v. Gumbs, 562 F. App. 110 (3d Cir. Mar. 28, 2014).

[148] United States v. Hamilton, 413 F.3d 1142 (10th Cir. 2005).

[149] United States v. Hampton, 504 F. App. 402 (6th Cir. Nov. 5, 2012).

[150] United States v. Harrell, 572 F. App. 452 (7th Cir. July 24, 2014).

[151] United States v. Hemetek, 393 F. App. 67 (4th Cir. Aug. 26, 2010).

[152] United States v. Henderson, 595 F.3d 1198 (10th Cir. Feb. 17, 2010).

[153] United States v. Hentzen, 638 F. App. 427 (6th Cir. Aug. 17, 2015).

[154] United States v. Hester, 627 F. App. 867 (11th Cir. Oct. 1, 2015).

[155] United States v. Hoffmann, 74 Military Justice 542 (N-M.C.C.A. Dec. 11, 2014).

[156] United States v. Houston, 665 F.3d 991 (8th Cir. Jan. 11, 2012).

[157] United States v. Howard, 766 F.3d 414 (5th Cir. Sept. 9, 2014).

[158] United States v. Howe, 545 F. App. 64 (2d Cir. Nov. 24, 2013).

[159] United States v. Hughes, 640 F.3d 428 (1st Cir. Apr. 8, 2011).

[160] United States v. Husman, 765 F.3d 169 (3d Cir. Sept. 3, 2014).

[161] United States v. Johnson, 537 F. App. 717 (9th Cir. Aug. 12, 2013).

[162] United States v. Johnson, 579 F. App. 920 (11th Cir. Sept. 16, 2014).

[163] United States v. Johnston, 789 F.3d 934 (9th Cir. May 26, 2015).

[164] United States v. Joubert, 778 F.3d 247 (1st Cir. Feb. 11, 2015).

[165] United States v. Kearney, 672 F.3d 81 (1st Cir. Feb. 29, 2012).

[166] United States v. Keith, 440 F. App. 503 (7th Cir. Oct. 4, 2011).

[167] United States v. Kernell, 667 F.3d 746 (6th Cir. Jan. 30, 2012).

[168] United States v. Killingbeck, 616 F. App. 14 (2d Cir. Oct. 5, 2015).

[169] United States v. Kinison, 710 F.3d 678 (6th Cir. Mar. 19, 2013).

[170] United States v. Koch, 625 F.3d 470 (8th Cir. Nov. 17, 2010).

[171] United States v. Konn, 634 F. App. 818 (2d Cir. Dec. 17, 2015).

[172] United States v. Kornhauser, 519 F. App. 41 (2d Cir. Mar. 26, 2013).

[173] United States v. Krueger, 809 F.3d 1109 (10th Cir. Nov. 10, 2015).

[174] United States v. Krupa, 658 F.3d 1174 (9th Cir. Feb. 7, 2011).

[175] United States v. Landsdown, 735 F.3d 805 (8th Cir. Nov. 7, 2013).

[176] United States v. Lanzon, 639 F.3d 1293 (11th Cir. May 4, 2011).

[177] United States v. Larman, 547 F. App. 475 (5th Cir. Nov. 13, 2013).

[178] United States v. Lebowitz, 676 F.3d 1000 (11th Cir. Apr. 5, 2012).

[179] United States v. Leet, 406 F. App. 830 (5th Cir. Nov. 19, 2010).

[180] United States v. Leon, 468 U.S. 897 (July 5, 1984).

[181] United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. June 18, 2015). United States v. Lovvorn, 524 F. App. 485 (11th Cir. July 25, 2013).

[182] United States v. Lowe, 795 F.3d 519 (6th Cir. July 28, 2015).

[183] United States v. Lynn, 636 F.3d 1127 (9th Cir. May 31, 2011).

[184] United States v. Majeroni, 784 F.3d 72 (1st Cir. Apr. 27, 2015).

[185] United States v. Manning, 738 F.3d 937 (8th Cir. Jan. 3, 2014).

[186] United States v. Martin, 297 F.3d 1308 (11th Cir. Jan. 29, 2002).

[187] United States v. McClellan, 792 F.3d 200 (1st Cir. July 6, 2015).

[188] United States v. McGlothlin, 391 F. App. 542 (7th Cir. July 28, 2010).

[189] United States v. McNealy, 625 F.3d 858 (5th Cir. Nov. 5, 2010).

[190] United States v. Merz, 396 F. App. 838 (3d Cir. Oct. 12, 2010).

[191] United States v. Miknevich, 638 F.3d 178 (3d Cir. Mar. 1, 2011).

[192] United States v. Moreland, 665 F.3d 137 (5th Cir. Dec. 14, 2011).

[193] United States v. Myers, 560 F. App. 184 (4th Cir. Mar. 10, 2014).

[194] United States v. Nance, 767 F.3d 1037 (10th Cir. Sept. 23, 2014).

[195] United States v. Needham, 718 F.3d 1190 (9th Cir. June 14, 2013).

[196] United States v. Norman, 448 F. App. 895 (11th Cir. Oct. 4, 2011).

[197] United States v. Oliver, 630 F.3d 397 (5th Cir. Jan. 6, 2011).

[198] United States v. Orisakwe, 624 F. App. 149 (5th Cir. Aug. 5, 2015).

[199] United States v. Oufnac, 449 F. App. 472 (6th Cir. Dec. 2, 2011).

[200] United States v. Pavulak, 700 F.3d 651 (3d Cir. Nov. 21, 2012).

[201] United States v. Pelland, 494 F. App. 475 (5th Cir. Oct. 17, 2012).

[202] United States v. Penton, 380 F. App. 818 (11th Cir. May 25, 2010).

[203] United States v. Pickett, 602 F. App. 774 (11th Cir. Mar. 16, 2015).

[204] United States v. Pires, 642 F.3d 1 (1st Cir. Apr. 6, 2011).

[205] United States v. Pirosko, 787 F. App. 358 (6th Cir. July 16, 2015).

[206] United States v. Plavcak, 411 F.3d 655 (6th Cir. June 6, 2005).

[207] United States v. Price, 582 F. App. 846 (11th Cir. Nov. 14, 2014).

[208] United States v. Pruitt, 638 F.3d 763 (11th Cir. Apr. 13, 2011).

[209] United States v. Ransfer, 749 F.3d 914 (11th Cir. Apr. 14, 2014).

[210] United States v. Raymonda, 780 F.3d 105 (2d Cir. Mar. 2, 2015).

[211] United States v. Reichling, 781 F.3d 883 (7th Cir. Mar. 27, 2015).

[212] United States v. Reiilly, 662 F.3d 774 (6th Cir. 2011).

[213] United States v. Rendon, 607 F.3d 982 (4th Cir. June 17, 2010).

[214] United States v. Renigar, 613 F.3d 990 (10th Cir. July 13, 2010).

[215] United States v. Reynolds, 626 F. App. 610 (6th Cir. Sept. 11, 2015).

[216] United States v. Richardson, 607 F.3d 357 (4th Cir. June 11, 2010).

[217] United States v. Robertson, 560 F. App. 626 (8th Cir. Mar. 20, 2014).

[218] United States v. Roetcisoender, 792 F.3d 547 (5th Cir. July 2, 2015).

[219] United States v. Rosa, 626 F.3d 56 (2d Cir. Oct. 27, 2010).

[220] United States v. Rose, 714 F.3d 362 (6th Cir. Apr. 18, 2013).

[221] United States v. Russo, 408 F. App. 753 (4th Cir. Jan. 21, 2011).

[222] United States v. Salva-Morales, 660 F.3d 72 (1st Cir. Oct. 31, 2011).

[223] United States v. Schaff, 454 F. App. 880 (11th Cir. Jan. 17, 2012).

[224] United States v. Schesso, 730 F.3d 1040 (9th Cir. Sept. 18, 2013).

[225] United States v. Schwinn, 376 F. App. 974 (11th Cir. Apr. 28, 2010).

[226] United States v. Sedaghaty, 728 F.3d 885 (9th Cir. Aug. 23, 2013).

[227] United States v. Seiver, 692 F.3d 774 (7th Cir. Aug. 28, 2012).

[228] United States v. Sensi, 542 F. App. 8 (2d Cir. Sept. 20, 2013).

[229] United States v. Seymour, 598 F. App. 867 (10th Cir. Mar. 27, 2015).

[230] United States v. Shelabarger, 770 F.3d 714 (8th Cir. Oct. 21, 2014).

[231] United States v. Sims, 603 F. App. 479 (6th Cir. Mar. 9, 2015).

[232] United States v. South, 359 F. App. 960 (11th Cir. Jan. 11, 2010).

[233] United States v. Springstead, 526 F. App. 168 (4th Cir. Apr. 15, 2013).

[234] United States v. Stanley, 533 F. App. 325 (4th Cir. July 19, 2013).

[235] United States v. Steele, 595 F. App. 208 (4th Cir. Dec. 24, 2014).

[236] United States v. Strausbaugh, 534 F. App. 178 (3d Cir. Aug. 9, 2013).

[237] United States v. Stringer, 739 F.3d 391 (8th Cir. Jan. 6, 2014).

[238] United States v. Suing, 712 F.3d 1209 (8th Cir. Apr. 10, 2013).

[239] United States v. Syed, 616 F. App. 973 (11th Cir. Sept. 17, 2015).

[240] United States v. Talley, 392 F. App. 129 (4th Cir. Aug. 9, 2010).

[241] United States v. Terry, 522 F.3d 645 (6th Cir. Apr. 15, 2008).

[242] United States v. Thomas, 788 F.3d 345 (2d Cir. June 11, 2015).

[243] United States v. Trepanier, 576 F. App. 531 (6th Cir. Apr. 13, 2014).

[244] United States v. Vallimont, 378 F. App. 972 (11th Cir. May 11, 2010).

[245] United States v. Vanbrackle, 397 F. App. 557 (11th Cir. Sept. 22, 2010).

[246] United States v. Vonneida, 601 F. App. 38 (2d Cir. Mar. 2, 2015).

[247] United States v. Walden, 478 F. App. 571 (11th Cir. May 3, 2012).

[248] United States v. Wellman, 663 F.3d 224 (4th Cir. Dec. 7, 2011).

[249] United States v. Westerlund, 477 F. App. 366 (6th Cir. Apr. 25, 2012).

[250] United States v. Wheelock, 772 F.3d 825 (8th Cir. Nov. 20, 2014).

[251] United States v. Williams, 592 F.3d 511 (4th Cir. Jan. 21, 2010).

[252] United States v. Winkler, 639 F.3d 692 (5th Cir. Apr. 25, 2011).

[253] United States v. Woerner, 703 F.3d 527 (5th Cir. Feb. 22, 2013).

[254] United States v. Wurie, 612 F. Supp. 2d 104 (2009).

[255] Ward, K. B. (2011). The plain (or not so plain) view doctrine: Applying the plain view doctrine to digital seizures. University of Cincinnati Law Review, 79(3), 1163-1187. https://doi.org/10.15779/Z38GS5N.

[256] Weinstein, J., & Drake, W. (2014). Public safety, privacy, and particularity: A new approach to search warrants for digital evidence. Electronic Commerce & Law Report, 19, 1-6. Who does what - judges. (n.d.). Retrieved November 10, 2015, from Inside the Federal Courts website: http://www.fjc.gov/federal/courts.nsf/autoframe?OpenForm&nav=menu5a&page=/federal/courts.nsf/page/304?opendocument.

[257] Wiesenberger, G. (1992). The Supreme Court and the interpretation of the federal rules of evidence. Ohio State Law Journal, 53(5), 1615-1639. Retrieved from http://hdl.handle.net/1811/64620.

[258] Williford v. Texas, 172 2004 Tex. App 309 (Court of Appeals of Texas, Eastland 2004). Wilson, C. (2011, July 11). Digital evidence dis-crepancies – Casey Anthony trial. Retrieved November 19, 2015, from Digital Detective website: http://www.digital-detective.net/digital-evidence-discrepancies-caseyanthony-trial/.

[259] Wilson, C. (2011, July 11). Digital evidence dis-crepancies: Casey Anthony trial [Blog post]. Retrieved from Digital Detective website: http://www.digital-detective.net/digital-evidence-discrepancies-caseyanthony-trial/.

[260] Yellon, A. (2009). The fourth amendment's new frontier: Judicial reasoning applying the fourth amendment to electronic communications. Journal of Business & Technology Law, 4(2), 411-437. Zappala, R. A. (2008). Evidence ESI

and the hearsay rule. 2008 FDCC winter meeting, pp. 2-5.

