

JUDICIAL CONFUSION AND THE DIGITAL DRUG
DOG SNIFF: PRAGMATIC SOLUTIONS PERMITTING
WARRANTLESS HASHING OF KNOWN ILLEGAL FILES

*Robyn Burrows**

INTRODUCTION

Matthew Mann was a lifeguard instructor for the Red Cross at a high school in Lafayette, Indiana.¹ One Saturday, a woman who was enrolled in the class discovered a towel concealing a video camera in the women's locker room.² When she and two other women rewound the tape and watched the video, they realized that Matthew Mann had videotaped himself installing the camera.³ The women alerted police and handed over the video camera.⁴ Days later, police obtained a search warrant permitting them to search Mann's home for video tapes, CDs, computers, or other electronic media for "images of women in locker rooms or other private areas."⁵

After police seized three computers and an external hard drive from Mann's home, they conducted a forensic examination⁶ of the digital evidence.⁷ Using a computer forensics program, Forensic Toolkit ("FTK"), Detective Huff made a copy of each hard drive and sorted through the computer files.⁸ FTK also contains a known file filter ("KFF") feature that uses

* George Mason University School of Law, J.D. Candidate, May 2012; Research Editor, GEORGE MASON LAW REVIEW, 2011-2012; Houghton College, B.A., Political Science, *summa cum laude*, December 2008. I would like to thank my family, especially my husband, for all their love and support.

¹ Brief of Appellant and Short Appendix at 4, *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010) (No. 08-3041); Brief of Plaintiff-Appellee at 3, *Mann*, 592 F.3d 779 (No. 08-3041).

² Brief of Appellant and Short Appendix, *supra* note 1, at 4.

³ *Id.*

⁴ *Id.*

⁵ *United States v. Mann*, 592 F.3d 779, 780-81 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010).

⁶ Computer forensics can easily be confused with electronic discovery, or eDiscovery. eDiscovery concerns the collecting and organizing of electronically stored information ("ESI") for litigation purposes. David R. Matthews, *EDiscovery Versus Computer Forensics*, 19 INFO. SECURITY J. 118, 118 (2010). Computer forensics can overlap with eDiscovery since forensics tools are often helpful when ESI has been deleted or modified. *Id.* Forensics experts, in contrast to eDiscovery practitioners, must additionally understand the intricate processes involved in creating, deleting, and modifying files. *Id.* at 119. Essentially, computer forensics is an investigation of electronic evidence even though the crime may not necessarily involve a computer. GEORGE MOHAY ET AL., *COMPUTER AND INTRUSION FORENSICS 3* (2003).

⁷ *Mann*, 592 F.3d at 781.

⁸ *Id.*

hashing, a mathematical algorithm,⁹ to determine if the hash values of files on the suspect's computer match the hash values of known illegal files contained in the software's database.¹⁰ Huff used the KFF feature, which subsequently flagged hundreds of files of child pornography on Mann's computers.¹¹ Mann moved to suppress the images of child pornography, arguing that Huff exceeded the scope of the warrant when he used KFF to identify evidence of an unrelated crime.¹² The court nevertheless held that Huff's use of KFF absent specific warrant authorization was permissible.¹³

In Mann's case, the alleged crime of voyeurism was not drastically different than the crime of possessing child pornography. The Seventh Circuit's holding, however, opens the door for police to use forensics tools like KFF to search for evidence of child pornography when the alleged crime is completely unrelated. According to the holding in *United States v. Mann*,¹⁴ police could use KFF to search for child pornography on a suspect's computer even if the warrant only contained probable cause for a white collar crime, like tax evasion. Since using KFF and its associated hashing process involves no privacy violations, police should be able to use this forensics tool in order to combat child exploitation.¹⁵

Despite the Seventh Circuit's holding, police may still face obstacles in convincing courts that tools like KFF are not creating the digital equivalent of a general warrant. For example, it is unclear whether the Seventh Circuit understood the difference between FTK and KFF when giving the green light to warrantless KFF.¹⁶ Had the Seventh Circuit understood the difference between FTK and its separate utility tool, KFF, it may have ruled as the Ninth Circuit did a year prior to the *Mann* decision. In 2009, the Ninth Circuit stated that the government's "sophisticated hashing tools" cannot be used absent a warrant.¹⁷ Further, in 2008, a federal district court from the Middle District of Pennsylvania held that hashing constitutes a search,¹⁸ eliminating the possibility of warrantless KFF. While KFF functions similarly to a drug dog sniff by only revealing the presence or absence

⁹ A hash analysis or hashing refers to the forensic process of comparing a file's digital fingerprint to a database of digital fingerprints in order to find a match. MOHAY ET AL., *supra* note 6, at 71-72.

¹⁰ Reply Brief of Appellant at 3, *Mann*, 592 F.3d 779 (No. 08-3041).

¹¹ *Mann*, 592 F.3d at 781.

¹² Brief of Appellant and Short Appendix, *supra* note 1, at 16, 24-25 (noting that "KFF Alert" files typically contain child pornography (internal quotation marks omitted)).

¹³ *Mann*, 592 F.3d at 784.

¹⁴ 579 F.3d 779 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010).

¹⁵ Assuming there is also a valid seizure.

¹⁶ *See infra* Part II.A.

¹⁷ *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (per curiam).

¹⁸ *United States v. Crist*, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008).

of contraband,¹⁹ the novel context of digital evidence investigations may prevent courts from fully embracing warrantless hashing without some sort of compromise.

Mann further demonstrates the importance to law enforcement of hashing tools like KFF. For example, police may never have been able to establish probable cause to search Mann's computers for child pornography, but by conducting a hash analysis while in possession of a valid warrant, they were able to uncover another one of Mann's disturbing predilections. Modern child pornographers, like Mann, are easily able to commit crimes and avoid detection by using computers.²⁰ The anonymity that the Internet provides, along with the opportunity for criminals to associate with others like themselves, reinforces deviant behavior and provides a safe haven for predation.²¹ In fact, half of all computer crimes involve the exploitation of children.²² Unlike thirty years ago, computers have large storage capacities and can download files quickly with fast Internet connections, leading to an increase in new criminal cases.²³

This Comment concludes that courts should permit warrantless hashing and discusses compromises that will assure courts that this technology is not subverting the Fourth Amendment. Part I explains hashing and computer investigations, the particularity requirement, and searches revealing only contraband. Further, Part I describes the apparent circuit split between the Ninth and Seventh Circuits as well as a federal district court's decision regarding hashing. Part II questions whether the Seventh Circuit in *Mann* truly split with the Ninth Circuit's decision in *United States v. Comprehensive Drug Testing, Inc.*²⁴ Part II also describes *United States v. Crist*²⁵ and

¹⁹ See, e.g., *United States v. Place*, 462 U.S. 696, 707 (1983) ("A 'canine sniff' by a well-trained narcotics dog . . . discloses only the presence or absence of narcotics, a contraband item.").

²⁰ See *MOHAY ET AL.*, *supra* note 6, at 2 ("[A]n essential, freely accessible, and widely used Internet can be adapted for every conceivable purpose, no matter how many laws are passed to regulate it.").

²¹ MONIQUE MATTEI FERRARO ET AL., *INVESTIGATING CHILD EXPLOITATION AND PORNOGRAPHY: THE INTERNET, THE LAW AND FORENSIC SCIENCE* 9 (2005) ("If the coming of the Internet has not exactly legalized child pornography of the most worrisome kind, then it has made such material extraordinarily accessible, and almost risk-free to those viewing it." (quoting Philip Jenkins, *Bringing the Loathsome to Light*, *CHRON. HIGHER EDUC.* (Wash., D.C.), Mar. 1, 2002, at B16)).

²² *Id.* at 4.

²³ *Id.* at 11-13. Computer forensics has been extremely helpful to police in cracking down on computer crimes. In 1998, computer forensic experts helped bring down an international child pornography ring, the "Wonderland Club." *MOHAY ET AL.*, *supra* note 6, at 119 (internal quotation marks omitted). As the Wonderland Club demonstrates, forensics experts are increasingly more important since predators are easily able to hide contraband among the thousands of files on a computer. Derek Regensburger, *Bytes, Balco, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in United States v. Comprehensive Drug Testing, Inc.*, 97 J. CRIM. L. & CRIMINOLOGY 1151, 1161 (2007).

²⁴ 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam).

²⁵ 627 F. Supp. 2d 575 (M.D. Pa. 2008).

its failed attempt to categorize hashing as a search. Lastly, Part II argues that courts should not require warrant authorization for hashing since it is not a search. As Professor Richard Salgado pointed out prior to *Crist*, hashing is likely not a search because it only exposes contraband, particularly since the hash value does not describe characteristics of the file input.²⁶

Despite not being a search, courts unfamiliar with hashing may be hesitant to allow its warrantless use since the hashing context is more complicated than the drug-sniffing dog in *Illinois v. Caballes*²⁷ or *United States v. Place*.²⁸ As a result, Part III suggests three pragmatic solutions to encourage courts to treat hashing as the digital equivalent of a drug-sniffing dog. First, courts could adopt a rule requiring police to submit a case log whenever they seek to introduce evidence from tools like KFF. The case log would document everything an investigator did while using the forensic software.²⁹ This requirement would function like an exclusionary rule, suppressing any evidence that is not accompanied by a case log. Second, courts could require that hashing be conducted on-site. Just as an individual is present during a traffic stop involving a drug dog sniff, an individual would be present as investigators run the hashing software on his computer. Lastly, police could visually demonstrate hashing in the courtroom by recreating the investigation before the judge and jury. These solutions hopefully represent temporary concessions until courts are fully comfortable with warrantless hashing.

I. BACKGROUND

This Part describes the steps a forensic examiner would take in conducting a digital evidence investigation and how hashing fits into the process. Further, it reviews the apparent circuit split between the Ninth and Seventh Circuits regarding warrantless hashing as well as *Crist*'s determination that hashing constitutes a search. Finally, this Part discusses searches revealing only contraband and the Fourth Amendment's particularity requirement.

²⁶ Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 42-43 (2006).

²⁷ 543 U.S. 405 (2005).

²⁸ 462 U.S. 696 (1983).

²⁹ AccessData Corp., *Forensic Toolkit: Sales and Promotional Summary*, at 7, available at http://www.accessdata.com/media/en_us/print/techdocs/Forensic%20Toolkit.pdf [hereinafter *Forensic Toolkit*].

A. *The Typical Computer Forensics Investigation*

A forensic examination of a hard drive is an exacting process. Courts must be assured that no information has been changed in the course of the investigation.³⁰ Lawyers today are quicker to raise evidentiary challenges to digital evidence since it is becoming more common in courts.³¹ As a result, an examiner must carefully document each step of the process in order to fulfill the “chain of custody” requirements,³² which prove that no cross-contamination has occurred.³³

In general, there are four ways a digital investigation can be performed: an examiner can (1) search the computer and print out a hard copy of the necessary files; (2) search the computer and make an electronic copy of the necessary files; (3) make an electronic copy of the hard drive on-site; or (4) seize the computer and do an analysis off-site at a laboratory.³⁴ At each step of the investigation, the examiner must document his every action.³⁵ When he arrives to the site, he will first photograph all evidence, including the computer screen containing the date and time.³⁶ If the investigation will be performed off-site, he should disconnect the power cable from the back of the computer before transporting the evidence.³⁷

³⁰ See, e.g., CHRIS PROSISE & KEVIN MANDIA, *INCIDENT RESPONSE & COMPUTER FORENSICS* 200 (2d ed. 2003).

³¹ FERRARO ET AL., *supra* note 21, at 215 (“Although courts were somewhat lenient in the past, as more judges and attorneys become familiar with digital evidence, more challenges are being raised relating to evidence-handling procedures.”).

³² Steven M. Abrams with Philip C. Weis, *Knowledge of Computer Forensics Is Becoming Essential for Attorneys in the Information Age*, N.Y. ST. B. ASS’N J., Feb. 2003, at 8, 9 (noting that examiners must follow “industry-established procedures” when carrying out an investigation). Chain of custody is defined as: “[A]ll of the steps that evidence has taken from the time it is located at the crime scene to the time it’s introduced in the courtroom. All steps include collection, transportation, analysis, and storage processes.” MICHAEL G. SOLOMON ET AL., *COMPUTER FORENSICS JUMPSTART* 60 (2005).

³³ Michael Harrington, “A Methodology for Digital Forensics”, 7 T.M. COOLEY J. PRAC. & CLINICAL L. 71, 72 (2004) (emphasizing the need to create a “forensically sterile” image).

³⁴ COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP’T OF JUSTICE, *SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS* 72, 77-78 (3d ed. 2009), available at <http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf>.

³⁵ MOHAY ET AL., *supra* note 6, at 77-79.

³⁶ *Id.* at 77.

³⁷ *Id.* at 78. If a computer is running Microsoft Windows, pulling the power supply plug from the back of the computer will preserve crucial information like the last user login, login time, and most recently used documents. NAT’L INST. OF JUSTICE, U.S. DEP’T OF JUSTICE, *ELECTRONIC CRIME SCENE INVESTIGATION: AN ON-THE-SCENE REFERENCE FOR FIRST RESPONDERS* 19 (2009), available at <http://www.ncjrs.gov/pdffiles1/nij/227050.pdf>. But see J. Philip Craiger, *Computer Forensics Procedures and Methods*, in 2 *HANDBOOK OF INFORMATION SECURITY: THREATS, VULNERABILITIES, PREVENTION, DETECTION, AND MANAGEMENT* 718 (Hossein Bidgoli ed., 2006) (noting that unplugging

The examiner must next image the hard drive.³⁸ During the imaging process, the examiner will first boot up the computer.³⁹ Yet, even turning on an individual's computer will alter files and render the evidence tainted.⁴⁰ Instead of booting up a computer by simply pressing the "power" button and allowing the computer to turn on as usual, an examiner will boot the system in a controlled manner, using a specialized boot diskette or CD.⁴¹ After he properly boots the system, the examiner uses a write blocker in order to ensure that system files are not altered.⁴² A properly imaged hard drive is important because it allows an examiner to later conduct a search without compromising the integrity of the original hard drive.⁴³

Once imaged, the examiner can begin his analysis of the copy.⁴⁴ At this point, the imaged drive will likely be loaded into a forensic software suite like FTK by AccessData Group, LLC or EnCase by Guidance Software, Inc., both of which can perform a variety of functions.⁴⁵ These programs "index" the imaged hard drive by organizing files into a searchable format.⁴⁶ Using FTK or EnCase, an examiner can perform keyword searches, recover deleted material, flag encrypted files, and analyze altered files.⁴⁷

Computer investigations, as opposed to traditional searches, are unique because they involve two levels—a physical analysis and a logical analysis.⁴⁸ The examiner conducts a physical analysis by extracting and preparing

a computer is no longer a "hard-and-fast rule" since it may cause police to lose important information, like running network connections and RAM contents).

³⁸ MOHAY ET AL., *supra* note 6, at 79. EnCase and FTK can be used to make an image. Abrams with Weis, *supra* note 32, at 10.

³⁹ MOHAY ET AL., *supra* note 6, at 79.

⁴⁰ *Id.* at 44. By simply turning on a computer, significant changes occur. For instance, Microsoft Windows may complete registry updates or decompress files which changes the file timestamps. *Id.*

⁴¹ *Id.*

⁴² *Id.* at 45.

⁴³ Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based On Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1233 (2004).

⁴⁴ Harrington, *supra* note 33, at 74.

⁴⁵ BILL NELSON ET AL., *GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS* 123 (2d ed. 2006).

⁴⁶ AccessData Corp., Product Information on AccessData Software Forensic Toolkit—(FTK), at 1, <http://www.jesc.co.za/downloads/products/1%20AccessData/10%20FTK%20Information.pdf> (last visited Sept. 20, 2011) [hereinafter Product Information on FTK] ("FTK will identify or 'index' all the files and group them together according to file header in a database so that the investigator can easily locate the files of interest."); EnCase, Product Information on EnCase Forensic—Transform Your Investigations, <http://www.guidancesoftware.com/WorkArea/DownloadAsset.aspx?id=671> (last visited Sept. 20, 2011).

⁴⁷ Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 327 (2010).

⁴⁸ Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 544 (2005).

data for investigation.⁴⁹ This often includes uncovering hidden data since criminals may attempt to hide information by partitioning the hard drive.⁵⁰ During a physical analysis, an examiner would combine all partitions on a drive and determine whether taken together they are smaller than the drive's capacity.⁵¹ If so, the suspect may have hidden information.⁵² Similarly, an examiner would look for deleted material—often the most valuable evidence.⁵³ To do so, the examiner uses “file carving” or “data carving” to recover files and file fragments.⁵⁴

A logical analysis is based on the file systems on the hard drive or the evidence that was produced after completing the physical analysis.⁵⁵ During a logical analysis, an examiner looking for evidence from pictures could search for all files with a “.jpg” extension⁵⁶ or conduct searches using keywords and phrases.⁵⁷ Additionally, an examiner could search for people's names, e-mail addresses, or any list of phrases or words that police provide as relevant to the warrant.⁵⁸ EnCase additionally allows searches by size and date of file creation.⁵⁹

B. *How a Hash Analysis Works*

In general, “[h]ashing is the process of taking computer data as a string of information, processing this string through a specially designed mathematical function that transposes each character of the string into another character or symbol, and converts it to another (usually smaller) string known as the hash value.”⁶⁰ A hash function is based on three fundamental principles: (1) the function must easily convert digital information into a fixed hash value; (2) it must be impossible to derive any information about the input from the hash value; and (3) it must be impossible for two differ-

⁴⁹ FERRARO ET AL., *supra* note 21, at 195.

⁵⁰ *Id.* at 198; *see* MOHAY ET AL., *supra* note 6, at 79.

⁵¹ FERRARO ET AL., *supra* note 21, at 197-98.

⁵² *Id.*

⁵³ *Id.* at 200.

⁵⁴ *Id.* at 201.

⁵⁵ Kerr, *supra* note 48, at 544.

⁵⁶ *Id.*

⁵⁷ MOHAY ET AL., *supra* note 6, at 79; Gaetano Ferro et al., *Electronically Stored Information: What Matrimonial Lawyers and Computer Forensics Need to Know*, 23 J. AM. ACAD. MATRIMONIAL L. 1, 35 (2010) (“Keyword searching is generally the most efficient method of combing through vast amounts of textual data on a given hard drive.”).

⁵⁸ Harrington, *supra* note 33, at 74.

⁵⁹ *See id.*

⁶⁰ Stephen Hoffman, *An Illustration of Hashing and Its Effect on Illegal File Content in the Digital Age*, INTELL. PROP. & TECH. L.J., Apr. 2010, at 6, 6. In simpler terms, hashing allows an examiner to convert a file into a number. Ralph C. Losey, *Hash: The New Bates Stamp*, 12 J. TECH. L. & POL'Y 1, 13 (2007).

ent inputs to have the same hash value.⁶¹ Using a forensics software program like EnCase or FTK, an investigator can create a hash value, which is like a “digital fingerprint” or “signature” of each file on an individual’s computer.⁶² The entire process is done without altering the original information.⁶³ Message Digest 5 (“MD5”) is a 128-bit hash algorithm that creates a hash value based on the unique bit-by-bit makeup of the file.⁶⁴ MD5 is the most commonly used algorithm for calculating hash values.⁶⁵ Essentially, “[t]he MD5 hash is an algorithm that, when applied to a set of data such as an original evidence file, produces a message digest or numerical ‘fingerprint.’”⁶⁶ Hashing is unique because the hash value is created based on the individual data, but it is impossible to produce the data based on the hash value.⁶⁷ For that reason, simply knowing a file’s hash value is of little use since it cannot reveal any information about the file.⁶⁸

Hash values are so unique that altering even one binary digit will change the value.⁶⁹ As a result, it is an extremely rare case where two files would have the same hash value, producing a “collision.”⁷⁰ While collisions are possible mathematically and have occurred in laboratory situations, in reality, they are extremely unlikely.⁷¹ In fact, the chances of two inputs or files having the same hash value is “one in 340 billion, billion, billion, billion.”⁷² The uniqueness of a hash value⁷³ is the reason why hashing is often

⁶¹ Hoffman, *supra* note 60, at 7 (citing AccessData, MD5 Collisions: The Effect on Computer Forensics 2 (2006), http://www.accessdata.com/media/en_US/print/papers/wp.MD5_Collisions.en_us.pdf).

⁶² Harrington, *supra* note 33, at 73.

⁶³ JAMES MICHAEL STEWART, SECURITY +: FAST PASS 120 (2004).

⁶⁴ *Id.* A “bit,” or “binary digit,” is defined as “[t]he smallest element of computer storage.” *Definition of: Bit*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=bit&i=38671,00.asp (last visited Sept. 20, 2011).

⁶⁵ FERRARO ET AL., *supra* note 21, at 197. Some computer forensics experts recommend an alternative 160 bit algorithm, SHA-1, although it calculates hash values much more slowly than MD5. *E.g.*, MICHAEL A. CALOYANNIDES, PRIVACY PROTECTION AND COMPUTER FORENSICS 253 (2d ed. 2004); Losey, *supra* note 60, at 14 (stating that SHA-1 is more reliable and effective than MD5).

⁶⁶ FERRARO ET AL., *supra* note 21, at 275.

⁶⁷ STEWART, *supra* note 63, at 120.

⁶⁸ *Id.* (“Thus, if someone obtains your hash value, they won’t be able to re-create the original data that produced the hash.”).

⁶⁹ DEBRA LITTLEJOHN SHINDER, SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK 379 (Ed Tittel ed., 2002). By simply deleting the first frame of a video clip, approximately 0.04 seconds worth of material, Stephen Hoffman shows that the file’s hash value is completely changed. Hoffman, *supra* note 60, at 10. Since hash values can be dramatically altered by changing even a small amount of data, Hoffman argues that predators will be able to change a single pixel of child pornography in order to evade hashing software. *Id.* As a result, hashing software may have the unintended consequence of encouraging criminals to evolve technologically faster than police. *Id.* at 11.

⁷⁰ See AccessData, MD5 Collisions: The Effect on Computer Forensics 2 (2006), http://www.accessdata.com/media/en_US/print/papers/wp.MD5_Collisions.en_us.pdf.

⁷¹ See *id.*

⁷² Harrington, *supra* note 33, at 73.

used in forensic investigations to ensure that the hash of the original hard drive matches the duplicate copy.⁷⁴ As a result, courts have generally accepted the reliability of hashing and allow expert testimony regarding it.⁷⁵

In addition to validating data, hashing increases the efficiency of forensic investigations. Most computers contain many harmless files, like operating system files, which are unnecessary to search in a criminal investigation.⁷⁶ Since computer investigations are often extremely time consuming, this efficient sorting system speeds up the process.⁷⁷ File-signature-recognition software can filter these files out and eliminate them from examination.⁷⁸ This same technology has been useful in cracking down on child pornography.⁷⁹ For example, the National Drug Intelligence Center (“NDIC”) created Hashkeeper, a database containing MD5 hash values of known child pornography.⁸⁰ Law enforcement can use databases like Hashkeeper to compare the hash values of a suspect’s files to the hash values of known child pornography files.⁸¹

This “hash matching” process can be performed using FTK’s KFF utility⁸² or EnCase’s signature analysis capabilities.⁸³ AccessData updates the KFF database with hash values of known files, including both ignorable program files and illegal files.⁸⁴ Once FTK processes the evidence, an overview screen will report whether the software identified any KFF Alert files.⁸⁵ KFF is an optional tool within FTK and an investigator must select

⁷³ Hoffman, *supra* note 60, at 7 (describing the “uniqueness theory” upon which the principle of hashing is based).

⁷⁴ STEWART, *supra* note 63, at 120. Once an examiner images a hard drive, he will hash both the original hard drive and the forensic image in order to determine if the hashes are the same. Craiger, *supra* note 37, at 720. If all values match, the digital copy is a guaranteed image of the original. *Id.*

⁷⁵ See, e.g., Sanders v. State, 191 S.W.3d 272, 278 (Tex. Ct. App. 2006) (upholding an examiner’s testimony regarding MD5 and its use in validating a copy of the imaged drive); see also Losey, *supra* note 60, at 20 (“Hash[ing] . . . has been accepted as reliable . . . by courts throughout the country.”).

⁷⁶ MOHAY ET AL., *supra* note 6, at 141.

⁷⁷ See Craiger, *supra* note 37, at 725 (noting that even straightforward investigations where police know what they are looking for can take half of a day).

⁷⁸ Robinton, *supra* note 47, at 326-27. The National Software Reference Library at <http://www.nsl.nist.gov> contains a database of both “known good” and “known bad” files which can help law enforcement conduct more efficient investigations. *Project Overview*, NAT’L SOFTWARE REFERENCE LIBR., http://www.nsl.nist.gov/Project_Overview.htm (last visited Sept. 20, 2011).

⁷⁹ Wade Davies, *Computer Forensics: How to Obtain and Analyze Electronic Evidence*, CHAMPION, June 2003, at 30, 35.

⁸⁰ MOHAY ET AL., *supra* note 6, at 153.

⁸¹ ROBERT MOORE, *SEARCH AND SEIZURE OF DIGITAL EVIDENCE* 58 (2005).

⁸² *Forensic Toolkit*, *supra* note 29, at 4.

⁸³ MOHAY ET AL., *supra* note 6, at 67-68.

⁸⁴ NELSON ET AL., *supra* note 45, at 396. The Known File Filter (“KFF”) is only a feature of FTK, not any other forensic software suites. *Id.* at 360.

⁸⁵ See V. J. Motto, *Accessing Evidence with FTK*, VINCE’S PLACE (2004), <http://www.vincesplace.com/courses/cst271/labs/AccessData01/AccessData01.htm>.

“KFF Lookup” before beginning his examination in order for the software to either filter out ignorable files or flag illegal files.⁸⁶

C. *The Fourth Amendment and Its Application to Digital Evidence*

The Fourth Amendment was based on the American colonists’ experience with the British government’s use of general warrants to search and seize an individual’s property without probable cause.⁸⁷ The framers consequently included the Fourth Amendment in the Bill of Rights in order to ensure that every warrant would be issued with probable cause, particularity, and reasonableness.⁸⁸ In the context of warrantless hashing, the concern is that police are able to find evidence of an unrelated crime without first having probable cause and a warrant, issued on the basis of that probable cause, particularly describing the evidence to be seized.⁸⁹ As a result, the police search may become analogous to a general warrant. Whether warrantless hashing is actually analogous to a general warrant will turn on whether hashing is a search, or whether the software reveals more than just contraband files.

1. Expectations of Privacy in Contraband

The Supreme Court has held that individuals do not have an “expectation of privacy” in contraband.⁹⁰ In *United States v. Jacobsen*,⁹¹ employees of a private freight carrier found a damaged package containing a white, powdery substance.⁹² The employees tested the substance and discovered it

⁸⁶ *Id.* (displaying FTK’s “Processes to Perform” dialog box, which offers options like hashing, KFF, HTML file listing, and full-index hashing); *see also* AccessData, FTK 2.2, Forensic Toolkit User Guide, at 77, <http://accessdata.com/downloads/media/ftkug.pdf> (last visited Sept. 20, 2011) (displaying FTK 2.2 and its “Evidence Processing” screen, which allows an examiner to select “KFF”).

⁸⁷ *See* Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 123 (2007).

⁸⁸ *Id.* at 124. Searches without a warrant are per se unreasonable. *Katz v. United States*, 389 U.S. 347, 357 (1967).

⁸⁹ *See* Brief of Appellant and Short Appendix, *supra* note 1, at 15 (“By running KFF and viewing the ‘KFF Alert’ files, Detective Huff treated the warrant as a general authorization to search Mann’s computers for evidence of crimes unrelated to voyeurism. Warrants must describe the objects to be seized with sufficient particularity to prevent a general exploratory rummaging in a person’s belongings.” (quoting *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999)) (internal quotation marks omitted)).

⁹⁰ *United States v. Jacobsen*, 466 U.S. 109, 122-23 & n.22 (1984) (noting that “governmental conduct that can reveal whether a substance is cocaine, and no other arguably ‘private’ fact, compromises no legitimate privacy interest”).

⁹¹ 466 U.S. 109 (1984).

⁹² *Id.* at 111.

was cocaine.⁹³ The Court held that a warrant was not required to execute a field test because it could only reveal whether the substance was cocaine and could not identify if the powder was an innocent substance, like sugar or talcum powder.⁹⁴ The Court noted that a “legitimate” expectation of privacy must be one that society is prepared to accept as reasonable.⁹⁵ Just as a burglar would not be entitled to an expectation of privacy over his stolen goods, an individual does not have an expectation of privacy in possessing illegal drugs.⁹⁶

Based on *Jacobsen*, the Supreme Court gave its blessing to dog sniffs revealing only contraband.⁹⁷ The Court in *Place* held that a drug dog sniff was not considered a search under the Fourth Amendment because its limited nature did not require police to “rummag[e]” through the suspect’s luggage and the dog only signaled the handler if drugs were present.⁹⁸ The Court recognized the uniqueness of a dog sniff, noting that it was “*sui generis*” and, therefore, not a search.⁹⁹ The Court confronted another dog sniff scenario in *Caballes* where police stopped a suspect for speeding.¹⁰⁰ While the officer was writing a ticket, a second officer walked a narcotics dog alongside the suspect’s car.¹⁰¹ The dog alerted the officer when it sniffed the driver’s trunk, indicating the presence of marijuana.¹⁰² Since *Place* held that a drug dog sniff was not a search, the Court held that police did not need a reasonable suspicion that the driver possessed drugs in order to use a drug dog.¹⁰³

In contrast to *Place* and *Caballes*, the Supreme Court in *Kyllo v. United States*¹⁰⁴ determined that a search occurred when police used a thermal imaging device to determine whether the heat emanating from the defendant’s home was higher than his neighbors, possibly indicating that he was using heat lamps to grow marijuana.¹⁰⁵ Since the thermal imaging device was “not in general public use” and also disclosed private, legal activity within the home, the Court held that it violated the Fourth Amendment.¹⁰⁶

⁹³ *Id.* at 111-12.

⁹⁴ *Id.* at 122-23.

⁹⁵ *Id.*

⁹⁶ *See id.* at 123.

⁹⁷ *United States v. Place*, 462 U.S. 696, 707 (1983).

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Illinois v. Caballes*, 543 U.S. 405, 406-07 (2005).

¹⁰¹ *Id.* at 406.

¹⁰² *Id.*

¹⁰³ *Id.* at 408-09.

¹⁰⁴ 533 U.S. 27 (2001).

¹⁰⁵ *Id.* at 29-30.

¹⁰⁶ *Id.* at 38, 40. While hashing may not be in general public use, Paul Ham suggests that courts do not necessarily follow *Kyllo* and its “general public use” requirement. Paul Ham, *Warrantless Search and Seizure of E-mail and Methods of Panoptical Prophylaxis*, 2008 B.C. INTELL. PROP. & TECH. F. 90801, at *11 (2010), available at <http://bciprf.org/wp-content/uploads/2011/07/16-WARRANTLESS->

While individuals do not have an expectation of privacy in contraband, the Court will strictly analyze whether a device revealing that contraband simultaneously reveals an individual's private, legal activity.¹⁰⁷ While dogs passed the test, the man-made thermal imaging device did not.

2. The Particularity Requirement and Intermingled Document Problem

Warrants must describe with particularity the items to be searched¹⁰⁸ by stating the “generic class of items.”¹⁰⁹ This allows the executing officer to identify with reasonable certainty the relevant items to be seized.¹¹⁰ The level of particularity will often hinge on the facts of the case and the items to be searched.¹¹¹ Police conducting computer searches often face problems in fulfilling the particularity requirement because incriminating evidence can be intermingled with an individual's private files.¹¹²

Some courts do not require strict enforcement of the particularity requirement for computer searches because they recognize that police cannot predict exactly where the evidence will be located on the hard drive.¹¹³ Oth-

SEARCH-AND-SEIZURE-OF-E-MAIL-AND-METHODS-OF-PANOPTICAL-PROPHYLAXIS.pdf (“[O]ne might think that since the search and seize [sic] of private e-mails requires technology and techniques that may be outside of general public use, e-mail should be protected from warrantless search and seizure. Yet, cases such as [*Commonwealth v. Proetto*], 771 A.2d 823 (Pa. Super. Ct. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003),] conclude that this expectation is not one the courts will fulfill.”)

¹⁰⁷ See *Kyllo*, 533 U.S. at 38 (“The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider ‘intimate’; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on.”).

¹⁰⁸ *Stanford v. Texas*, 379 U.S. 476, 485 (1965); *Marron v. United States*, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”).

¹⁰⁹ *United States v. Horn*, 187 F.3d 781, 788 (8th Cir. 1999).

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² Allen H. Quist, Note, *Flexing Judicial Muscles: Did the Ninth Circuit Abandon Judicial Restraint in United States v. Comprehensive Drug Testing, Inc.*?, 24 BYU J. PUB. L. 371, 372-73 (2010).

¹¹³ See *United States v. Lacy*, 119 F.3d 742, 746-47 (9th Cir. 1997) (permitting a warrant using generic terms because a more specific description of the digital equipment was not feasible); *United States v. Hill*, 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004) (upholding a broad warrant since police were not required to sort the digital evidence on-site to determine which media contained child pornography), *aff'd*, 459 F.3d 966 (9th Cir. 2006); *Frasier v. State*, 794 N.E.2d 449, 465-66 (Ind. Ct. App. 2003) (holding that an officer could open all files in order to determine their contents, regardless of file labels); *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (holding that police were entitled to search all files to determine if they were within the scope of the warrant). Courts may loosely enforce the particularity requirement as applied to computers because the Supreme Court has held that “officers are not required to use the least intrusive technique when conducting a search.” G. Robert

er courts require police to specify which files or media types they will search.¹¹⁴ Predicting the course of an investigation, however, can be impossible since police do not always know what types of challenges they will face.¹¹⁵ A suspect may attempt to hide an incriminating picture by changing the “.jpg” extension to “.doc” or “.wpd.”¹¹⁶ This may force police to search the entire computer in order to find a hidden file. Professor Orin Kerr likened this situation to searching an “entire digital haystack to find the needle.”¹¹⁷ For example, in *United States v. Grimm*,¹¹⁸ the court noted that “a computer search ‘may be as extensive as reasonably required to locate the items described in the warrant.’”¹¹⁹ In *Grimm*, the court upheld a broad warrant that allowed police to obtain “any [computer] equipment” and any computer software.¹²⁰ Similarly, the court in *State v. Hinahara*¹²¹ held that the particularity requirement was not violated when police searched a suspect’s entire hard drive in order to find images of child pornography.¹²²

D. *The Apparent Circuit Split Regarding Warrantless Hashing*

When *Mann* was handed down in 2010, two new splits developed between the Ninth and Seventh Circuits. First, *Mann* rejected the Ninth Circuit’s approach to the plain view doctrine, refusing to completely throw out the plain view doctrine in digital evidence cases.¹²³ Second, at least one

McLain, Jr., Note, *United States v. Hill: A New Rule, But No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1090 (2007).

¹¹⁴ See *United States v. Riccardi*, 405 F.3d 852, 862-63 (10th Cir. 2005) (requiring warrants to specifically name files and media types to be searched); *In re Search of 3817 W. W. End*, 321 F. Supp. 2d 953, 962 (N.D. Ill. 2004) (requiring police to provide a search protocol before searching digital evidence).

¹¹⁵ See Regensburger, *supra* note 23, at 1162, 1206.

¹¹⁶ *Id.* at 1161 (citing Kerr, *supra* note 48, at 544-45).

¹¹⁷ Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 304 (2005). Kerr suggests that this difficulty could be remedied by allowing forensic examiners, rather than judges, to craft the scope of the search. Kerr, *supra* note 48, at 575-76.

¹¹⁸ 439 F.3d 1263 (10th Cir. 2006).

¹¹⁹ *Id.* at 1270 (quoting *United States v. Wuagneux*, 683 F.2d 1343, 1352 (11th Cir. 1982)).

¹²⁰ *Id.* (alteration in original) (internal quotation marks omitted) (quoting the search warrant at issue).

¹²¹ 166 P.3d 1129 (N.M. Ct. App. 2007).

¹²² *Id.* at 1135.

¹²³ *United States v. Mann*, 592 F.3d 779, 785 (7th Cir.) (“Although the Ninth Circuit’s rules provide some guidance in a murky area, we are inclined to find more common ground with the dissent’s position that jettisoning the plain view doctrine entirely in digital evidence cases is an ‘efficient but overbroad approach.’” (quoting *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1013 (9th Cir. 2009) (Callahan, J., concurring in part and dissenting in part), *superseded by* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam))), *cert. denied*, 130 S. Ct. 3525 (2010).

scholar noted that *Mann* appeared to permit warrantless hashing.¹²⁴ In contrast, the Ninth Circuit in *Comprehensive* requires specific warrant authorization.¹²⁵

In *Comprehensive*, federal authorities obtained a warrant to search ten baseball players' urine analysis records in order to investigate steroid use in professional baseball.¹²⁶ Despite the limited warrant, the government seized hundreds of players' records.¹²⁷ While this case did not involve hashing, the court generally discussed procedures for searching electronically stored information since it strongly disapproved of the government's actions.¹²⁸ As part of this discussion, the Ninth Circuit noted that "sophisticated hashing tools . . . that allow the identification of well-known illegal files" may not be used "without specific authorization in the warrant," which must be provided through probable cause.¹²⁹ While dicta, the court nevertheless strongly indicated that it would not tolerate anything but strict adherence to the warrant and the particularity requirement.¹³⁰

In contrast, *Mann* seems to allow warrantless hashing,¹³¹ although as later explained, the court's analysis conflates FTK and its utility tool, KFF.¹³² When women discovered that Matthew Mann had concealed a video camera in the women's locker room, police used FTK and KFF to perform a forensic analysis of Mann's computers.¹³³ KFF subsequently revealed hundreds of images of child pornography.¹³⁴ While the court chastised Detective Huff for opening four flagged KFF files, it held that Huff's use of FTK and KFF was within the scope of the warrant.¹³⁵ The court held that Huff's actions were reasonable "[b]ecause [he] discovered the child pornography while conducting a systematic search for evidence of voyeurism."¹³⁶ The court referenced the intermingled document problem and ar-

¹²⁴ See Michael M. O'Hear, *Seventh Circuit Clarifies Application of Fourth Amendment to Searches of Computer Hard Drives*, MARQUETTE U.L. SCH. FAC. BLOG (Jan. 22, 2010), <http://law.marquette.edu/facultyblog/2010/01/22/seventh-circuit-clarifies-application-of-fourth-amendment-to-searches-of-computer-hard-drives/> (noting that *Mann*'s holding regarding warrantless use of file filtering software broke with the Ninth Circuit's requirement that tools like KFF be accompanied by a warrant).

¹²⁵ *Comprehensive*, 579 F.3d at 999.

¹²⁶ *Id.* at 993.

¹²⁷ *Id.*

¹²⁸ *Id.* at 996-97.

¹²⁹ *Id.* at 999.

¹³⁰ In fact, "the Ninth Circuit considers dicta as binding in some instances." Bryan K. Weir, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 GEO. MASON U. C.R. L.J. 83, 117 n.254 (2010).

¹³¹ See *United States v. Mann*, 592 F.3d 779, 784 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010).

¹³² See *infra* Part II.A.

¹³³ *Mann*, 592 F.3d at 780-81.

¹³⁴ *Id.* at 781.

¹³⁵ *Id.* at 784-85.

¹³⁶ *Id.* at 786.

gued that images of women in locker rooms could be located virtually anywhere on Mann's hard drive, making it reasonable for Huff to use FTK and KFF.¹³⁷ The court ultimately denied Mann's suppression motion except as to the four flagged KFF files that Huff opened without a warrant.¹³⁸

E. *Crist and Its Attempt to Define Hashing as a Search Based on "Government Review"*

While *Mann* and *Comprehensive* discussed hashing, neither explicitly analyzed whether hashing constituted a search but rather operated on the assumption that a warrant was necessary.¹³⁹ In contrast, a federal district court in *United States v. Crist* held that hashing is a search requiring warrant authorization.¹⁴⁰ In *Crist*, defendant Robert Crist argued for the suppression of child pornography found on his computer.¹⁴¹ When Crist stopped paying rent, his landlord cleared Crist's possessions from the house and gave his computer to a friend, Seth Hipple.¹⁴² As Hipple was cleaning the computer up for his own use, he came across videos containing child pornography.¹⁴³ Hipple subsequently handed the computer over to police.¹⁴⁴ A forensic analyst then created a hash index of the hard drive using EnCase.¹⁴⁵ The analyst compared the hash values on Crist's computer to the hash values of known child pornography, which resulted in a discovery of 171 illicit videos.¹⁴⁶

The government argued that the hash analysis within EnCase was not a search because the investigators "didn't look at any files, they simply accessed the computer."¹⁴⁷ The court upheld Crist's motion to suppress, finding that the "running of hash values" constituted a search and that the EnCase examination exceeded the scope of Hipple's private search.¹⁴⁸ Interes-

¹³⁷ *Id.* at 784 ("Given the nature of Detective Huff's search and the fact that Mann could have images of women in locker rooms virtually anywhere on his computers, there is no reason to believe that Detective Huff exceeded the scope of the warrant by employing the FTK software without more.")

¹³⁸ *Id.* ("Detective Huff knew (or should have known) that files in a database of known child pornography images would be outside the scope of the warrant to search for images of women in locker rooms—presumably images that Mann himself had captured.")

¹³⁹ For example, *Mann* never explicitly discussed whether hashing was a search, but assumed it was since its reasoning hinged on whether using FTK and KFF exceeded the scope of the warrant. *Mann*, 592 F.3d at 782.

¹⁴⁰ *United States v. Crist*, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008).

¹⁴¹ *Id.* at 576.

¹⁴² *Id.* at 577.

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.* at 578.

¹⁴⁶ *Crist*, 627 F. Supp. 2d at 578.

¹⁴⁷ *Id.* at 585 (internal quotation marks omitted) (quoting trial transcript).

¹⁴⁸ *Id.* (internal quotation marks omitted).

tingly, the court conceptualized the computer as containing multiple compartments of platters or disks.¹⁴⁹ It then argued that EnCase was applied to “each compartment, disk, file, folder, and bit.”¹⁵⁰ The court argued that “[b]y subjecting the entire computer to a hash value analysis—every file, internet history, picture, and ‘buddy list’ became available for Government review.”¹⁵¹

II. ANALYSIS

Part II discusses the apparent circuit split between the Seventh and Ninth Circuits and why these circuits might not necessarily disagree on warrantless hashing. Further, Part II discusses *Crist*'s struggle with hashing technology and analyzes whether hashes identifying illegal files should be considered a search. This Comment suggests that while hashing is not a search, there are contextual differences that courts may find important in deciding whether to extend the principles of *Caballes* to digital investigations.

A. *Does Mann Really Hold that No Warrant Is Needed to Use Hashing Tools Which Identify Known Illegal Files?*

Since the Seventh Circuit assumed that hashing constituted a search, it was forced to rest its analysis on whether Huff's use of KFF remained within the scope of the warrant.¹⁵² The problem with the court's analysis is that it misunderstands how FTK and KFF function. The court seems to believe that KFF is simply part of running FTK. For example, in describing Huff's investigation, the court says that the “FTK software identified four ‘KFF Alert’ files and 677 ‘flagged thumbnails.’”¹⁵³ This language does not acknowledge that Huff had to make a separate decision to use KFF to identify known illegal files,¹⁵⁴ like the child pornography he supposedly “discovered.”¹⁵⁵ The court further demonstrates its confusion over the technology by stating: “[A]s to the use of the filtering software itself, Detective Huff used it to index and catalogue the files into a viewable format.”¹⁵⁶ The court misunderstands that the filtering software, KFF, does not index and cata-

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² *See supra* note 139.

¹⁵³ *United States v. Mann*, 592 F.3d 779, 781 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010).

¹⁵⁴ *See supra* note 86 and accompanying text.

¹⁵⁵ *Mann*, 592 F.3d at 786.

¹⁵⁶ *Id.* at 784.

logue files.¹⁵⁷ Instead, FTK performs indexing.¹⁵⁸ Rather than specifically ruling on warrantless KFF, the court conflated its analysis of FTK with the entirely separate issue of FTK's utility tool and treated FTK and KFF as one and the same.¹⁵⁹

After determining that Huff's use of "FTK software employing a filter" was valid, the court then cited to the Ninth Circuit's supposedly contrary approach which requires "specific authorization in the warrant" when using "sophisticated hashing tools . . . that allow the identification of well-known illegal files."¹⁶⁰ Yet it does not make sense for the Seventh Circuit to contrast its approach with the Ninth Circuit's specific view on KFF when *Mann* has not specifically addressed whether investigators can use KFF without a warrant.¹⁶¹ Instead of focusing on warrantless hashing, the court turns the case into an intermingled document problem¹⁶² by stating that it was reasonable to use FTK and KFF because evidence of voyeurism could be hidden anywhere on Mann's computer.¹⁶³

Interestingly, the court specifically acknowledged that KFF contains a database mostly consisting of known child pornography hash values.¹⁶⁴ The court nevertheless failed to realize that Huff was guaranteed to find evidence outside the scope of the warrant by using KFF.¹⁶⁵ Huff's search could only remain within the scope of the warrant if KFF could alert him to known voyeurism files. The court does not understand that KFF, an optional tool, could only help Huff find evidence of another crime. Had the court been correctly informed, it may have required warrant authorization for hashing, just as the Ninth Circuit did. For example, the court refused to

¹⁵⁷ See Forensic Toolkit, *supra* note 29, at 4.

¹⁵⁸ Product Information on FTK, *supra* note 46, at 1.

¹⁵⁹ Timothy Ceder appears to use similar language as the court, stating that Huff used FTK "to convert all the images into a viewable format, which included listing 'Known File Filter . . . Alerts.'" Timothy C. Ceder, Note, *The Guidelines of Comprehensive Drug Testing, Inc.: A Measured Approach?*, 89 OR. L. REV. 351, 376-77 (2010).

¹⁶⁰ *Mann*, 592 F.3d at 784 (alteration in original) (quoting *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 999 (9th Cir. 2009), *superseded by* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam)) (internal quotation marks omitted).

¹⁶¹ See *id.* at 782.

¹⁶² See *supra* Part.I.C.2.

¹⁶³ *Mann*, 592 F.3d at 782-83 ("Undoubtedly the warrant's description serves as a limitation on what files may reasonably be searched. The problem with applying this principle to computer searches lies in the fact that such images could be nearly anywhere on the computers."); see also Scott D. Blake, *Let's Be Reasonable: Fourth Amendment Principles in the Digital Age*, 5 SEVENTH CIRCUIT REV. 491, 517 (2010) ("Therefore, the court held that it was reasonable for the detective to both use the FTK software program and briefly examine all files on the computer in order to determine their contents.").

¹⁶⁴ *Mann*, 592 F.3d. at 781, 784.

¹⁶⁵ Essentially, Huff was looking in an area that could not produce evidence of the alleged crime. "For example, '[i]f you are looking for an adult elephant, searching for it in a chest of drawers is not reasonable.'" Blake, *supra* note 163, at 496 (alteration in original) (quoting *Platteville Area Apartment Ass'n v. City of Platteville*, 179 F.3d 574, 579 (7th Cir. 1999)).

always require “pre-approval” for forensics tools “tailored to uncovering evidence that is responsive to a properly circumscribed warrant.”¹⁶⁶ If KFF cannot uncover evidence of voyeurism, it cannot produce evidence “responsive” to a warrant for voyeurism.¹⁶⁷ As a result, the court would likely require pre-approval for KFF since it will almost always reveal unrelated criminal activity.¹⁶⁸

The court’s confusion over FTK and KFF is of little surprise considering the government’s argument. Rather than explaining that KFF is a separate function within FTK, the government referred to the “files alerted in the FTK alert.”¹⁶⁹ In fact, nowhere in its brief did the government ever mention “KFF” or “known file filter.” Whenever it mentioned Huff’s hashing, it referred to FTK.¹⁷⁰ Based on the government’s description of the forensic process, the court did not understand that using FTK did not necessarily entail KFF. Such misinformation led the court to believe it was splitting with the Ninth Circuit when the court might have ruled otherwise if it understood the forensic software.

The government’s focus on the plain view doctrine also indicates that it wanted to avoid directly addressing KFF.¹⁷¹ It argued that the plain view doctrine applied to the “files alerted in the FTK alert” because Huff never abandoned his search for images of women in locker rooms, and because he immediately identified the alert files as child pornography.¹⁷² Further, the government argued that Huff did not act outside the scope of the warrant when using FTK because, under the plain view doctrine, the officer’s subjective intent is irrelevant.¹⁷³ Essentially, “[a]s long as the officer’s search was within the scope of the warrant, an officer could intend to find one

¹⁶⁶ *Mann*, 592 F.3d at 785.

¹⁶⁷ See *supra* notes 78-86 and accompanying text.

¹⁶⁸ Of course, this is only the case if the Seventh Circuit also determines that KFF constitutes a search for Fourth Amendment purposes. See *supra* note 139.

¹⁶⁹ Brief of Plaintiff-Appellee, *supra* note 1, at 15.

¹⁷⁰ *Id.* at 4 (“FTK also provides an alert that the hard drive contains a certain number of files known to law enforcement.”); *id.* at 5 (“FTK provided an alert that it contained four files known to law enforcement.”); *id.* at 12 (“FTK did not turn Huff’s search into a general exploratory rummaging of Mann’s belongings. It identified only four files as containing material known to law enforcement.”); *id.* (“Mann also claims Detective Huff searched files on the Western Digital hard drive ‘where it was unlikely or impossible to find evidence of voyeurism’ because FTK had identified certain files as containing evidence of other crimes unrelated to the warrant.” (quoting Brief of Appellant and Short Appendix, *supra* note 1, at 18)).

¹⁷¹ See Reply Brief of Appellant, *supra* note 10, at 1 (noting that the government was assuming that the plain view doctrine was the only relevant issue).

¹⁷² Brief of Plaintiff-Appellee, *supra* note 1, at 14-15 (“Thus, Huff was both lawfully present and legally entitled to access each file. . . . Once Huff clicked on an image, he did not have to read, study, manipulate or seek expert advice to determine its incriminating nature.”).

¹⁷³ *Id.* at 15. The court also argued that Huff remained within the scope of the warrant because the warrant permitted Huff to search all image files. *United States v. Mann*, 592 F.3d 779, 784 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010); Blake, *supra* note 163, at 518.

class of evidence even if the warrant authorizes a search only for another class of evidence.”¹⁷⁴

This argument fails, however, since Huff technically abandoned his search for voyeurism as soon as he chose to use a tool capable of identifying child pornography.¹⁷⁵ While the plain view doctrine does not require an inadvertent discovery,¹⁷⁶ the cases the government cited involve police searching an area that only *potentially* contained evidence of another crime.¹⁷⁷ In contrast, a KFF containing only hash values of child pornography will *only* produce evidence of child pornography,¹⁷⁸ an unrelated crime. Therefore, KFF cannot help police find files containing images of women in locker rooms but rather is only useful for identifying evidence of child pornography.

As Mann stated, Huff exceeded the scope of the warrant by “looking in areas where it was unreasonable if not impossible to find objects authorized by his warrant.”¹⁷⁹ Consequently, Mann argued that the warrant turned into a general search, divorced from the original allegation of voyeurism.¹⁸⁰ The court never fully grasped Mann’s gripe with KFF or the irrelevance of the plain view doctrine, perhaps because the government never explained that it only “stumb[ed] upon”¹⁸¹ the child pornography because Huff, by selecting “KFF Lookup” before beginning his examination, *instructed* the software to flag child pornography.¹⁸²

¹⁷⁴ Brief of Plaintiff-Appellee, *supra* note 1, at 15; *see also* Blake, *supra* note 163, at 518 (explaining that the court distinguished Huff’s subjective intent from the officer in *Carey* who testified that he began actively looking for child pornography after discovering the first image (citing *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999))).

¹⁷⁵ *See supra* notes 164-67 and accompanying text.

¹⁷⁶ *Horton v. California*, 496 U.S. 128, 137-41 (1990).

¹⁷⁷ *See* Brief of Plaintiff-Appellee, *supra* note 1, at 15-16 (citing *Horton*, 496 U.S. at 138-40, *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007), and *United States v. Barnes*, 909 F.2d 1059, 1069-70 (7th Cir. 1990)). *Horton* held that the plain view doctrine applied to an officer with a warrant to search a residence for stolen goods even though he testified that he was looking for “other evidence connecting petitioner to the robbery.” *Horton*, 496 U.S. at 131, 142. *Ning Wen* held that police could use evidence of an unrelated crime even though they expected to find such evidence. *Ning Wen*, 477 F.3d at 898. Finally, *Barnes* involved a situation where FBI agents searched a residence for cocaine but testified that they were also looking for fruits of the crime. *Barnes*, 909 F.2d at 1069 n.12. In each case, police were looking in an area that could produce evidence responsive to the warrant, even though they may have also expected to find evidence of an unrelated crime.

¹⁷⁸ *See supra* note 164 and accompanying text.

¹⁷⁹ Reply Brief of Appellant, *supra* note 10, at 1; *see also* Blake, *supra* note 163, at 517 (“Mann interpreted the warrant to be restrictive—only authorizing a search for ‘images of women in locker rooms and other private places.’” (quoting *United States v. Mann*, 592 F.3d 779, 782 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010))).

¹⁸⁰ Reply Brief of Appellant, *supra* note 10, at 14.

¹⁸¹ *Mann*, 592 F.3d at 783.

¹⁸² *See* Motto, *supra* note 85.

Perhaps the Seventh Circuit, like the Ninth, would have required specific warrant authorization for KFF if it had a clearer understanding of the hashing software. Assuming the court understood the software, it is nevertheless possible that it would have permitted the warrantless hashing based on the similarities between the alleged crime and possessing child pornography. The defendant in *Mann* was accused of voyeurism, a sex-related crime.¹⁸³ As a result, the Seventh Circuit could have reasoned that there was a close connection between the alleged crime of voyeurism and possessing child pornography, making it reasonable for Huff to use KFF. In fact, the court notes that given the nature of the search—images of women—it would be impossible to *not* run across existing child pornography.¹⁸⁴ In contrast, if Mann was accused of copyright infringement and Huff used KFF to flag child pornography, the court may have felt differently about using warrantless KFF. In such a situation, there would be absolutely no connection between the alleged crime and possessing child pornography.¹⁸⁵

B. *Crist's Struggle with Hashing*

Prior to the decision in *Mann*, a federal district court in *Crist* explicitly held that “the running of hash values” is a search.¹⁸⁶ The court reasoned that hashing exposed all of Crist’s files to “Government review.”¹⁸⁷ What exactly the court meant by “Government review” is unclear.¹⁸⁸ As the government argued, it did not look at any files¹⁸⁹ since the forensic software generated the hash values.¹⁹⁰ The court then continued its muddled analysis, saying that Crist’s privacy was violated more by the government’s hashing than by Hipple’s search.¹⁹¹ The court reasoned that Hipple only searched a fraction of the computer, while the government’s hashing tool “compromised . . . all the computer’s remaining contents.”¹⁹² The court’s illogical

¹⁸³ *Mann*, 592 F.3d at 780-81.

¹⁸⁴ *Id.* at 783.

¹⁸⁵ See *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that an officer’s search of child pornography photographs was unlawful even though the officer had a warrant to search the computer for photographic evidence of an unrelated crime—drug trafficking).

¹⁸⁶ *United States v. Crist*, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008) (internal quotation marks omitted).

¹⁸⁷ *Id.*

¹⁸⁸ Marcia Hofmann seems to agree that hashing exposes “data to which a client has a legitimate privacy interest.” Marcia Hofmann, *Arguing for Suppression of ‘Hash’ Evidence*, CHAMPION, May 2009, at 20, 22. Hofmann argues that hashing is an invasion of privacy since it “requires the government to access all data on a computer.” *Id.* at 23.

¹⁸⁹ See Losey, *supra* note 60, at 17 (“[E]ven the basic properties of the original file remain hidden.”).

¹⁹⁰ *Crist*, 627 F. Supp. 2d at 585.

¹⁹¹ *Id.* at 586.

¹⁹² *Id.*

holding, therefore, considers a search involving a human viewing both legal and illegal file contents less intrusive than a search that uses a computer algorithm to reveal only known contraband.¹⁹³

Whether a hash analysis is considered a search may also turn on whether one views a computer as a single container or a series of containers. The container analogy is particularly relevant since some view computers as a container “with a series of electronic ‘containers’ . . . that must be each separately opened,” therefore constituting a new search.¹⁹⁴ The court in *Crist* conceptualized a computer as a container within a container, with platters or disks representing the inner containers.¹⁹⁵ Accordingly, the court held that the hashing software accessed multiple platters and therefore was a search.¹⁹⁶

The analysis in *Crist* reflects the age-old “chicken versus the egg” question. Did the court in *Crist* consider hashing a search because it had adopted the view that a computer is a “container of containers”? Or, did it subsequently use this approach as a pretext because it intuitively felt that hashing was too invasive and needed a rationale to defeat the government’s warrantless hashing argument? The latter seems more likely based on the court’s skewed container analogy. While hard drives do write information to platters, platters are only a component of the hard drive.¹⁹⁷ In order for the hard drive to function, all platters must work together since data is written *across* platters.¹⁹⁸ It would have made more sense if the court had argued that each file was an individual container since files can be utilized separately, unlike a standalone platter. Based on this strange analysis, it appears that the court does not understand the technology involved, but nevertheless assumed that some invasion of privacy had occurred.¹⁹⁹

¹⁹³ See *id.* at 577 (noting that Hipple looked through a “bunch of songs” on *Crist*’s computer before finding the pornography (internal quotation marks omitted)).

¹⁹⁴ Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 240 (2005); see also Kerr, *supra* note 48, at 550.

¹⁹⁵ See *Crist*, 627 F. Supp. 2d at 585 n.7; see also Hofmann, *supra* note 188, at 24 n.23 (noting that some courts, like *Crist*, use the container-within-a-container approach); Marc Palumbo, Note, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 979 (2009) (“Importantly . . . *Crist* held that the individual platters—or smaller physical subsections of the hard drive—were analogous to closed containers. Accordingly, the court ruled that the government could not search an entire hard drive consisting of multiple platters.” (footnote omitted)).

¹⁹⁶ *Crist*, 627 F. Supp. 2d at 585.

¹⁹⁷ See Craiger, *supra* note 37, at 724.

¹⁹⁸ *Hard Disk Details(5)*, DATA RECOVERY BLOG (Nov. 28, 2008), <http://www.hddoctor.net/hard-disk-details-5/> (“Your data is NOT written on the top of one platter and when that gets full then written to the next platter. It is written across all the platters at the same time, making a cylinder of your data.”); see also Craiger, *supra* note 37, at 724 (describing a cylinder as a “column of two or more tracks on two or more platters”).

¹⁹⁹ Hofmann, *supra* note 188, at 22 (“Unfortunately, the court’s analysis is not very detailed and leaves important questions unanswered.”). Hofmann notes that *Crist* did not specifically answer when the search occurred. *Id.* For instance, the court did not say whether the hash analysis constituted one

Courts cannot be entirely blamed for such shortcomings, however, since the parties do not always appropriately educate judges. For example, Crist's brief emphasized EnCase's powerful forensic capabilities, like cracking passwords and recovering deleted material, even though hashing involves neither of these processes.²⁰⁰ Further, Crist sought to highlight the intrusiveness of EnCase by stating that "80,023,714,840 bytes were examined by the EnCase program."²⁰¹ The court subsequently believed that "the 'running of hash values'" exposed countless files, when in reality, EnCase was simply generating values that had no meaning to either the program or the examiner, aside from signaling a hash value match.²⁰²

The government's brief, in contrast, explained hashing more accurately. The government described how it imaged the computer and completed a hash analysis before it opened any files.²⁰³ By using EnCase's signature analysis capabilities, it "was virtually certain that at least five videotapes contained on the defendant's computer contained child pornography."²⁰⁴ Unfortunately, as much as the government emphasized that it did not look at a single file in order to determine the presence of child pornography, the court held that the scope of the government's search exceeded the scope of the private search.²⁰⁵

C. *Should a Hash Analysis Be Considered a Search?*

Prior to the decisions in *Mann*, *Comprehensive*, and *Crist*, Professor Richard Salgado concluded that using hashing to identify contraband files should not be considered a search under the Fourth Amendment.²⁰⁶ Salgado first distinguished hashing from the situation in *Arizona v. Hicks*.²⁰⁷ In *Hicks*, police officers investigating a shooting in an apartment moved a turntable in order to read and record the serial number on a stereo that they suspected was stolen.²⁰⁸ The Court held that the officer's moving of the

search or whether multiple searches occurred when the hard drive was removed, imaged, and hashed. *Id.* Further, Hofmann notes that *Crist* does not consider the drug dog cases that Salgado emphasizes. *Id.*

²⁰⁰ Reply Brief of Defendant, Robert Ellsworth Crist, III, in Response to the Government's Supplemental Brief Opposing Pretrial Motion to Suppress at 2, *Crist*, 627 F. Supp. 2d 575 (No. 1:07-cr-211).

²⁰¹ *Id.*

²⁰² See *Crist*, 627 F. Supp. 2d at 585.

²⁰³ Supplemental Brief Opposing Pre-Trial Motion to Suppress at 7, *Crist*, 627 F. Supp. 2d 575 (No. 1:07-cr-211).

²⁰⁴ *Id.* at 8.

²⁰⁵ *Crist*, 627 F. Supp. 2d at 585.

²⁰⁶ Salgado, *supra* note 26, at 39.

²⁰⁷ 480 U.S. 321 (1987).

²⁰⁸ *Id.* at 323.

stereo component constituted a search.²⁰⁹ Based on *Hicks*, officers seizing an item in plain view must have probable cause, which must also be “readily apparent.”²¹⁰ Since the officers in *Hicks* could not have known that the stereo was stolen without checking the serial number, there was no probable cause to seize the equipment.²¹¹

Salgado admits that hashing, at face value, appears similar to the police action in *Hicks* since calculating a hash value requires an investigator to access the suspect’s hard drive.²¹² A hash value is nevertheless different than the serial number on the stereo equipment since the serial number always existed while the hash value does not exist apart from the software program that produced it.²¹³ Unlike the serial number, police cannot “search” for a hash value since it must first be calculated.²¹⁴ Further, a hash value is unlike the turntable’s serial number, which helped police determine that the equipment was stolen, because a hash value does not disclose information about the individual file.²¹⁵

While the Supreme Court held that “[a] search is a search, even if it happens to disclose nothing but the bottom of a turntable,” a hash value is no more valuable than a random number.²¹⁶ For example, an investigator that sees a hash value of “162B6274FFEE2E5BD96403E772125A35”²¹⁷ cannot possibly determine a file’s contents using the MD5 sum.²¹⁸ Further, since the software program is responsible for detecting contraband, the examiner is only tangentially involved in the process.²¹⁹ Even if individuals have an expectation of privacy in their hash values, Salgado states that “the true degree of intrusion into private matters is, at most, de minimis.”²²⁰ Moreover, having an expectation of privacy in one’s hash values would require investigators to obtain a warrant simply to verify an imaged drive,

²⁰⁹ *Id.* at 325.

²¹⁰ STEPHEN A. SALTZBURG & DANIEL J. CAPRA, *AMERICAN CRIMINAL PROCEDURE: CASES AND COMMENTARY* 342 (8th ed. 2007); *see also Hicks*, 480 U.S. at 326.

²¹¹ *Hicks*, 480 U.S. at 326.

²¹² Salgado, *supra* note 26, at 42.

²¹³ *Id.*

²¹⁴ *See id.* (“A hash value . . . is something that the agent will derive . . .”).

²¹⁵ *Id.*

²¹⁶ *Hicks*, 480 U.S. at 325.

²¹⁷ Losey, *supra* note 60, at 2.

²¹⁸ STEWART, *supra* note 63, at 120.

²¹⁹ While Professor Hunt claims that there is no test that can only reveal contraband without requiring human interpretation, the computer software, or KFF, is responsible for the entire analysis. Cecil J. Hunt, II, *Calling in the Dogs: Suspicionless Sniff Searches and Reasonable Expectations of Privacy*, 56 CASE W. RES. L. REV. 285, 335 (2005). Perhaps hashing software, rather than drug dogs, deserves the “*sui generis* status.” *See id.* at 335-36 (emphasis added).

²²⁰ Salgado, *supra* note 26, at 42. “Because hashing is ‘minimally intrusive’ and is driven by ‘operational necessities,’ there is little constitutional significance.” *Id.* at 43. The only benefit law enforcement gains from obtaining hash values is in matching them to known contraband files. Ceder, *supra* note 159, at 371.

since hashing is also used to perform image verification.²²¹ This would produce an extremely inconvenient and convoluted result.²²²

Hashing is also unique because it can make digital investigations *less* intrusive. For example, hashing tools may be used to exclude duplicate files²²³ or evidence that the investigator is not interested in.²²⁴ The investigator can use a hash set for known, ignorable files to minimize the amount of files he views by filtering out common programs.²²⁵ In this regard, hashing actually reduces the risk of an investigator running into intermingled files.²²⁶ Since many courts already broadly construe search warrants for digital evidence, it would seem petty to restrict a forensics tool which narrowly targets the search and additionally aids police in putting child predators behind bars.²²⁷

The non-intrusiveness of hashing can further be demonstrated by comparing it to a similar forensic tool designed to ferret out child pornography. The newest version of FTK, FTK 3.1, comes equipped with “[e]xplicit image detection” (“EID”).²²⁸ Rather than identifying child pornography by comparing hash values, the EID analyzes *visual content*, particularly flesh colored tones in photographs.²²⁹ After the software visually analyzes the images, it assigns each image a number ranging from one to one hundred based on its probability of being pornographic.²³⁰ The software is essentially

²²¹ See *supra* note 74.

²²² Salgado believes that Professor Orin Kerr, based on his exposure theory, would find that individuals have an expectation of privacy in their hash values. Salgado, *supra* note 26, at 41-42. Under Kerr’s theory, a “search occurs when any data on a hard drive or information about that data, no matter how little, is exposed to human observation.” *Id.* (citing Kerr, *supra* note 48, at 547-48).

²²³ Losey, *supra* note 60, at 36-37 (referring to the process of removing duplicate files via hashing as “de-duplication”).

²²⁴ Salgado, *supra* note 26, at 41; see also *supra* notes 76-79 and accompanying text.

²²⁵ Losey, *supra* note 60, at 39.

²²⁶ Salgado, *supra* note 26, at 41 (“Using Professor Kerr’s terminology, the unwanted data is not ‘exposed’ in the forensics work.”).

²²⁷ See *United States v. Grimmer*, 439 F.3d 1263, 1270 (10th Cir. 2006) (upholding a warrant that permitted the search of any computer equipment creating/displaying computer data); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (holding that a warrant was not overbroad even though it did not restrict police to seizing only items relating to the suspect’s crimes); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (holding that the wholesale removal of computer equipment would have been permissible had the warrant specified the crime for which the computers were being seized); see also Katherine T. Kleindienst et al., *Computer Crimes*, 46 AM. CRIM. L. REV. 315, 324 (2009) (“Broad searches have been justified as ‘about the narrowest definable search and seizure reasonably likely to obtain the [evidence].’” (alteration in original) (quoting *Upham*, 168 F.3d at 535)); Trepel, *supra* note 87, at 126 (arguing that the scope of warrants authorizing searches of computers have become analogous to general warrants). Hashing has also been useful in hunting down child pornographers trading illicit files via peer-to-peer software sharing programs. Losey, *supra* note 60, at 28.

²²⁸ AccessData, FTK 3: Explicit Image Detection, http://accessdata.com/downloads/media/Explicit_Image_Detection.pdf (last visited Sept. 20, 2011).

²²⁹ *Id.*

²³⁰ *Id.*

acting as a human eye by actually looking at the user's file contents. Perhaps this is how the court in *Crist* envisioned hashing and why it subsequently deemed it a search. The EID would likely be considered a search because its process involves "looking" at the contents of files. Hashing nevertheless does not require the software to "see" anything, rendering the process much different than a traditional Fourth Amendment search.

Additionally, allowing warrantless hashing is not completely without precedent. Many courts have already accepted warrantless hashing in the context of file sharing programs, like LimeWire.²³¹ For example, in *United States v. Miknevich*,²³² police obtained a search warrant by establishing probable cause in part through a hash value match between a suspect's shared file and a hash value of known child pornography.²³³ While these file sharing cases are based on the premise that there is no objectively reasonable expectation of privacy when sharing files with the public, they nevertheless provide some precedence for allowing warrantless hashing.²³⁴ If warrantless hashing is already being conducted to supply probable cause for warrants, it is not such a great step to extend warrantless hashing to a situation where a valid warrant already exists, albeit a warrant related to another crime.

There are also strong similarities between the drug-sniffing dog in *Caballes* and hashing, as Salgado suggested.²³⁵ Both the dog and the software alert the "handler" only when something illegal is detected.²³⁶ Hashing is actually much more accurate than a dog sniff since it is almost mathematically impossible to mistake one file for another.²³⁷ Since the Supreme Court has held that individuals do not have a legitimate expectation of privacy in

²³¹ See *United States v. Willard*, No. 3:10-CR-154, 2010 WL 3784944, at *3 (E.D. Va. Sept. 20, 2010); *State v. Tremaine*, 315 S.W.3d 769, 773 (Mo. Ct. App. 2010); *State v. Lyons*, 9 A.3d 596, 598 (N.J. Super. Ct. App. Div. 2010).

²³² 638 F.3d 178 (3d Cir. 2011).

²³³ *Id.* at 183.

²³⁴ See *United States v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008).

²³⁵ Salgado, *supra* note 26, at 45.

²³⁶ While Marcia Hofmann criticized Salgado's comparison, her analysis contains the same type of confusion present in *Crist*. Hofmann argues that hashing and a dog sniff would only be comparable if the dog needed to search through the entire container's contents. Hofmann, *supra* note 188, at 22. This would be correct if the forensic analyst needed to view the files in order to calculate the hash values. Instead, a computer autonomously does this. Further, the hashing software does not recognize or report the contents of the files it hashes. See Losey, *supra* note 60, at 17 (describing hashing as maintaining the secrecy of a computer's files).

²³⁷ Losey, *supra* note 60, at 15 (emphasizing how extremely rare a collision is). Drug-sniffing dogs frequently make mistakes in identifying contraband. Hunt, *supra* note 219, at 328-29 ("Thus, an alert by a drug-sniffing dog, does not necessarily indicate the presence of contraband. Rather, it simply indicates the mere possibility that the container being searched might contain contraband.").

contraband²³⁸ and hashing only reveals the presence of contraband, it follows that police should be able to conduct warrantless hashing.²³⁹

D. *If Hashing Is Not a Search, Why Would Courts Be Hesitant to Apply Caballes's Principles to Digital Evidence?*

Despite the soundness of Salgado's argument, there are contextual differences between the dog sniff in *Caballes* and hashing. Justice Ginsburg's dissent in *Caballes* argues in part that the introduction of a police dog would transform the traffic stop into an adversarial encounter.²⁴⁰ Even if Ginsburg exaggerates the presence of a drug dog, it is still possible that an investigator's hash analysis of a defendant's hard drive could appear more intrusive than a dog sniffing the outside of a bag.²⁴¹ In the case of a drug dog sniff, a layman can understand that dogs have a heightened sense of smell and that the dog is trained to detect specific substances. In contrast, few people, including judges, have the technological background in computer forensics to understand hashing. Besides the intimidating technological complexities, hash analyses also differ from a dog sniff since the examination of digital evidence often requires the suspect's computer to not only be searched, but taken off-site.²⁴² The off-site investigation may require days to complete.²⁴³ In contrast, a drug dog encounter only lasts as long as the dog's few seconds of sniffing.

²³⁸ See *supra* Part I.C.1.

²³⁹ While some commentators take issue with using "contraband sensing devices" absent a warrant, this Comment only considers situations where police already have a warrant to search and seize a suspect's digital evidence. See John M. Junker, *The Structure of the Fourth Amendment: The Scope of the Protection*, 79 J. CRIM. L. & CRIMINOLOGY 1105, 1108-09 (1989) ("Thus, to be within the scope of the fourth amendment, the moving party must establish that government agents have engaged in a search or seizure that affected such party's undefeased legitimate expectation of privacy in his or her person, house, papers or effects."). Consequently, warrantless hashing would only occur after police obtain probable cause to search and seize an individual's electronic storage device for evidence of a crime. Police could not scan people's computers at random. See *id.* at 1140 (predicting a future where police randomly use "futuristic devices" to scan anyone for contraband). Even those who disagree with the analysis in *Caballes* argue that dog sniffs for contraband are acceptable as long as the car is already lawfully seized. See Hunt, *supra* note 219, at 334.

²⁴⁰ *Illinois v. Caballes*, 543 U.S. 405, 421 (2005) (Ginsburg, J., dissenting) ("Injecting such an animal into a routine traffic stop changes the character of the encounter between the police and the motorist. The stop becomes broader, more adversarial, and (in at least some cases) longer.").

²⁴¹ This feeling of intrusiveness may also be a result of the sheer amount of personal information people store on their computers. See Robinton, *supra* note 47, at 321 ("In a world where computers facilitate and store oceans of data about every aspect of our lives, it seems certain that some type of crime can always be found among the bits and bytes of the average hard drive.").

²⁴² Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 86-87 (2005).

²⁴³ *Id.* at 94.

Further, using a drug dog absent a warrant likely raises fewer suspicions since no one would ever accuse a dog of possessing ulterior motives. Yet suspicions are aroused in a situation where humans create the forensic tool and its hash database, and then are entrusted to correctly run the software.²⁴⁴ While Salgado is correct in determining that hashing is not a search, courts will likely be weary of permitting warrantless hashing without safeguards that ensure it is not invading individuals' expectations of privacy.

III. PRAGMATIC SOLUTIONS ENCOURAGING COURTS TO PERMIT WARRANTLESS HASHING

While hashing should not qualify as a search under the Fourth Amendment, it may be too idealistic to believe that courts will accept this argument. It may require time and compromises until courts are comfortable with tools like KFF and can accept that their warrantless use does not invade privacy interests. This Comment suggests three pragmatic solutions that allow warrantless hashing while keeping in mind possible judicial concerns: (1) create a suppression rule for hashing tools identifying known illegal files; (2) conduct the hash analysis on-site; and (3) demonstrate hashing in court.

A. *Creating a Suppression Rule for Hashing Tools Identifying Known Illegal Files*

In order to assure courts that hashing is not eroding individuals' expectations of privacy in their computers, courts could require case logs to accompany any evidence that the hash analysis reveals. For example, FTK allows investigators to turn on a case log which "document[s] . . . activities during the investigation and analysis."²⁴⁵ Choosing to use the case log is simple as FTK creates it automatically.²⁴⁶ When using FTK on a new case, the examiner would choose what he wanted the case log to include.²⁴⁷ A window opens that allows the user to select various events to log, including

²⁴⁴ Salgado appears to anticipate this problem: "It would seem that populating a hash set requires exercise of discretion that is not required when teaching a dog to detect cocaine or developing a chemical test to react to particular narcotics." Salgado, *supra* note 26, at 46. Another commentator argues that there is "[f]ar greater potential for police abuse . . . with a tool that targets individual documents than with a test that reveals an illegal chemical compound." Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1205 (1995).

²⁴⁵ AccessData, Forensic Toolkit User Guide, at 10, http://www.accessdata.com/media/en_us/print/manuals/FTK1UsersGuide.pdf (last visited Sept. 20, 2011).

²⁴⁶ *Id.*

²⁴⁷ *Id.* at 60.

case and evidence events, error messages, bookmarking events, searching events, data carving, and Internet searches.²⁴⁸ FTK's Processing Files form also allows the examiner to log extended information like indexing and hashing.²⁴⁹

Most established forensics companies would be smart to use the case log function as it enhances witness credibility by backing up a witness's memory with a solid record of investigation.²⁵⁰ File Hound, a free forensic tool for law enforcement, is developing a case log report that creates "play-by-play documentation of all the steps an investigator has taken" while using the software.²⁵¹ Case logs are particularly important in a case lasting months or even years.²⁵² Foretech, a company which offers eDiscovery and computer forensics services, ensures clients that a case log will be used to maintain a solid chain of evidence.²⁵³ Each case log includes the date and time of evidence acquisition, names of examiners, search queries, investigator notes, Internet searches, and computer and hard drive serial numbers.²⁵⁴

Case logs are most similar to a forensic examiner's report, which may be entered into evidence at court.²⁵⁵ In the report, an examiner describes his findings, conclusions, and opinions on the evidence discovered,²⁵⁶ including any relevant text or images.²⁵⁷ While the examiner's report is intended to produce a "repeatable standard," much like how the case log retraces an examiner's steps, it nevertheless depends on the examiner's memory and diligence in documenting as he investigates.²⁵⁸ Further, the report serves a much broader purpose than a case log since it explains why and how the

²⁴⁸ *Id.* at 64.

²⁴⁹ *Id.* at 132.

²⁵⁰ Foretech, White Paper, Forensic Lifecycle: An Effective and Repeatable Process for Computer Forensic Investigations, at 16, <http://www.foretech.com/documents/ForensicLifeCycleWhitePaper.pdf> (last visited Oct. 2, 2010).

²⁵¹ Wm. Blair Gillam & Marc Rogers, File Hound: A Forensics Tool for First Responders, at 4 (Aug. 18, 2005) (unpublished manuscript), available at http://www.dfrws.org/2005/proceedings/gillam_filehound.pdf.

²⁵² Foretech, *supra* note 250, at 16.

²⁵³ *Id.* at 9.

²⁵⁴ *Id.* at 9, 16.

²⁵⁵ Ferro et al., *supra* note 57, at 36-37; Mark Maher, *Becoming a Forensic Investigator*, SANS INST., at 8 (Aug. 9, 2004), http://www.sans.org/reading_room/whitepapers/forensics/forensic-investigator_1453. The report writer would typically testify in court to authenticate the evidence found during the course of the investigation. See PROSISE & MANDIA, *supra* note 30, at 200 ("You meet the demands of authentication by ensuring that whomever collected the evidence is a matter of record.")

²⁵⁶ Maher, *supra* note 255, at 5. The point of the report is to "persuade the court that [the examiner's] findings are sound." Ferro et al., *supra* note 57, at 36-37.

²⁵⁷ FERRARO ET AL., *supra* note 21, at 277; Ferro et al., *supra* note 57, at 37 (noting that the report should include screenshots of the investigation).

²⁵⁸ Maher, *supra* note 255, at 2 (describing how an examiner must discipline himself to document his steps in order and document his opinions as soon as they are formed).

computer was analyzed as well as the examiner's findings and conclusions.²⁵⁹

A case log would also function similarly to a police officer's dashboard-mounted camera as evidence in court. Police cameras have been helpful in determining whether a police officer had reasonable suspicion to detain a suspect²⁶⁰ or whether an officer was justified in prolonging a traffic stop.²⁶¹ For example, even though an officer may claim that a suspect was acting nervous, the court may come to the opposite conclusion after watching the video and determining that the suspect was actually acting in a calm manner.²⁶² While video evidence is often compelling in court, it cannot always capture important details.²⁶³ For example, a police camera may not be facing the correct direction²⁶⁴ or an officer's conversation with a suspect may be difficult to hear because the camera's microphone could not pick it up.²⁶⁵ In contrast, a case log captures every action an examiner takes while using the forensic software.²⁶⁶ Since video evidence has been helpful in solving traditional Fourth Amendment cases despite its shortcomings, it follows that case logs would be extremely helpful in recreating a digital investigation so the court can judge the appropriateness of the authorities' action.

Courts could adopt a rule that would require case logs to accompany flagged files that a hash analysis tool like KFF identified. Unless police enter a case log into evidence, courts could suppress evidence of unrelated illegal activity. The case log would add a layer of accountability and oversight that would ensure courts that technology is not being used to cut corners on individuals' privacy. One expert's comments reveal why case logs would be particularly important to courts skeptical of digital investigations:

[Y]ou might not want the log feature turned on. Make sure you're aware of the implications before you begin. Many times during an investigation, you follow a lead or gut reaction instead of being systematic. If opposing attorneys were to see such log files, they might question your technique. It's better to find the items, and then perform a systematic search with the log file feature turned on. This approach isn't meant to conceal evidence, but to show that the results are consistently reproducible.²⁶⁷

²⁵⁹ *Id.*

²⁶⁰ *See* *United States v. Freeman*, 412 F. App'x 735, 736-37 (6th Cir. 2010).

²⁶¹ *See* *United States v. Jackson*, 517 F. Supp. 2d 859, 877-78 (W.D. La. 2007), *report and recommendation adopted by* No. 06-50170-01, 2007 WL 2461602.

²⁶² *See id.*

²⁶³ *See* *McCann v. Hood*, No. 1:07-cv-519-SEB-JMS, 2009 WL 276792, at *1 (S.D. Ind. Feb. 3, 2009).

²⁶⁴ *E.g., id.*

²⁶⁵ *See* *Bradford v. Wiggins*, 516 F.3d 1189, 1192 (10th Cir. 2008).

²⁶⁶ Forensic Toolkit, *supra* note 29, at 6.

²⁶⁷ NELSON ET AL., *supra* note 45, at 361.

With a case log, an investigation is out in the open and a judge does not need to question whether an examiner's search wandered away from the warrant based on a "gut reaction." Case logs would also strengthen digital evidence since they would represent an unbiased account of the search, unlike potentially skewed testimony from a police officer.²⁶⁸ The case log may be enough to convince courts like *Crist* and *Comprehensive* that hashing is not subjecting the contents of a suspect's computer to "Government review."

A requirement that case logs be presented to the court would likely satisfy even *Comprehensive*, which established somewhat burdensome, prophylactic guidelines for computer searches.²⁶⁹ While the rules in *Comprehensive* are criticized,²⁷⁰ they nevertheless embrace the possibility of warrantless hashing with a case log rule. One of the Ninth Circuit's rules require independent third parties to complete segregation and redaction of data.²⁷¹ Once the segregation and redaction is complete, the government may then only search for information the warrant authorizes.²⁷² If the Ninth Circuit is comfortable with the government using independent third parties to sort through digital evidence, it should have no problem using an independent third party to also review a case log in order to confirm that the government's warrantless hashing did not subject the suspect's entire computer to review. The third party would be able to testify in court and describe, based on the case log, exactly what actions the government took within the software suite.

B. *Performing the Hash Analysis On-Site*

Even if courts are provided case logs from a forensic investigation, they may still be reluctant to extend *Caballes* to hashing. Courts will likely take issue with one of the greatest differences between hashing and the drug dog sniff: An individual is present during a drug dog sniff while most forensic examinations occur off-site.²⁷³ The presence of an individual is not

²⁶⁸ As a result, case logs would present reduced opportunities for "[t]estifying," which occurs when police provide false testimony against a defendant in court. SALTZBURG & CAPRA, *supra* note 210, at 331-32.

²⁶⁹ *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009), *superseded by* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam).

²⁷⁰ See Blake, *supra* note 163, at 493 (describing the Ninth Circuit's rules as "premature," "impractical," and "unnecessary"); Quist, *supra* note 112, at 394 ("Thus, as prophylactic dicta, the guidelines represent an attack on the common law approach to jurisprudence.").

²⁷¹ *Comprehensive*, 579 F.3d at 1006; Weir, *supra* note 130, at 103 ("The second restriction requires the magistrate to order the intermingled information to be separated by specialized personnel or an 'independent third party' under court supervision or deny the warrant altogether.").

²⁷² *Comprehensive*, 579 F.3d at 1000.

²⁷³ COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 34, at 76.

trivial since he acts as a check on police action. A driver undergoing a drug dog sniff during a traffic stop is able to observe the dog sniffing his property. He can also ensure that the officer is not rummaging through his belongings and exceeding the scope of his authority.

Courts may be willing to accept warrantless hashing if its context is more like the drug dog sniff. If a hash analysis is conducted on-site, suspects would have the opportunity to observe the hash analysis and actually see that police are not viewing their files or gathering any information, aside from flagged KFF files. While KFF may be confusing to describe, seeing the software in action may alleviate concerns. Technology is often not as intuitive as a simple dog sniff. Therefore, courts and suspects alike may be more comfortable taking small steps in applying traditional Fourth Amendment principles to the hashing context.

Forensic investigations may be performed on-site or off-site. Only the Ninth Circuit requires the affidavit to explain why an off-site analysis is necessary.²⁷⁴ Searching is often conducted off-site because it can take a considerable amount of time to find what police are looking for on a computer containing potentially ten million pages of information.²⁷⁵ An examiner may need weeks or months to complete an analysis of just one hard drive.²⁷⁶ Files may be encrypted or an analyst may need to reconstruct files in order to view their contents.²⁷⁷ On-site searches may also be too burdensome because they can risk damaging evidence.²⁷⁸ For example, if a computer is connected to the Internet, there is a possibility that an individual with remote access could destroy evidence.²⁷⁹ Removing the search to an off-site location ensures that the investigation will proceed in a controlled environment.²⁸⁰ In some situations, however, on-site searches are preferable, especially if the computer system is small and the search scope is narrow.²⁸¹ If only a few computers need to be searched and if only certain types of files (like e-mail or picture files) are the target of the search, the search may be completely executed on site.²⁸²

²⁷⁴ See *id.* at 78. In contrast, the Eleventh Circuit has held that warrants do not need to contain an off-site search protocol in order to satisfy the particularity requirement of the Fourth Amendment. *United States v. Khanani*, 502 F.3d 1281, 1290-91 (11th Cir. 2007).

²⁷⁵ COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 34, at 77; see also Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 53 (2001-2002) (noting that an off-site analysis is sometimes needed because criminals may rig their computers to self-destruct if anyone other than an expert working in a controlled environment attempts to search them).

²⁷⁶ Kerr, *supra* note 48, at 544.

²⁷⁷ *Id.* at 545-46.

²⁷⁸ COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 34, at 77.

²⁷⁹ *Id.* at 78.

²⁸⁰ *Id.* at 77.

²⁸¹ Brenner & Frederiksen, *supra* note 275, at 71.

²⁸² *Id.* at 71-72.

Police also have a choice of whether to image a hard drive on-site or off-site, although imaging must be done on-site if the warrant does not permit seizure of the hardware.²⁸³ Imaging on-site may also be necessary if the individual requires access to his computer for business purposes and removing the entire computer off-site would be disruptive.²⁸⁴ When imaging must be performed off-site, forensic processes like indexing and hashing would typically also occur off-site since imaging must be completed first to ensure the integrity of the evidence.²⁸⁵

If police must image the hard drive off-site yet want to run a tool like KFF on-site, technology exists which makes this possible. Voom Technologies, Inc., a computer forensics manufacturer, created the Shadow 2, a hardware device which “provides investigators with read write access from the host computer’s perspective, while maintaining the original hard drive unchanged.”²⁸⁶ While imaging can take hours to complete, depending on the size of the suspect’s hard drive,²⁸⁷ the Shadow instead allows investigators to boot and run a suspect’s computer without compromising evidence and without necessitating imaging.²⁸⁸ Unlike a write-blocker which can only read data, the Shadow can actually operate the suspect’s computer without slowing it down.²⁸⁹

David Biessener, Voom’s CEO, stated that a forensics examiner can utilize the Shadow to hash the suspect’s hard drive without first imaging it.²⁹⁰ This can be done repeatedly without ever changing the original data.²⁹¹

²⁸³ MOHAY ET AL., *supra* note 6, at 49; *see also Materials on Electronic Discovery: Search and Seizure of Computers and Data in Criminal Cases*, FED. JUD. CENTER, 3, 8 (Dec. 8, 2004), [http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi31.rtf/\\$file/ElecDi31.rtf](http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi31.rtf/$file/ElecDi31.rtf) (follow “Comprehensive set of definitions and procedures for the seizure of computers and data, conducting off-site searches of computers and data, and searching computers of an ongoing business enterprise” hyperlink) (noting that authorities must first attempt to image digital evidence if the warrant does not permit a seizure, but if imaging on-site is impracticable or impossible, authorities can seize digital equipment).

²⁸⁴ *See* *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 437-38 (W.D. Tex. 1993) (pointing out that investigators could have imaged the digital media within hours rather than seizing the company’s computers and disrupting business), *aff’d*, 36 F.3d 457 (5th Cir. 1994).

²⁸⁵ *See* SHINDER, *supra* note 69, at 597 (noting that the first step in an investigation is to image the hard drive).

²⁸⁶ *What is the Shadow 2?*, DIGITAL INTELLIGENCE, <http://www.digitalintelligence.com/products/shadow2/> (last visited Sept. 20, 2011).

²⁸⁷ Craiger, *supra* note 37, at 722.

²⁸⁸ *What is the Shadow 2?*, *supra* note 286.

²⁸⁹ Voom Techs., Inc., Voom Shadow 2 Details, at 2, <http://www.voomtech.com/downloads/Shadow2/DetailedDes.pdf> (last visited Aug. 27, 2011).

²⁹⁰ E-mail from David Biessener, CEO of Voom Techs., Inc., to Robyn Burrows (Nov. 5, 2010, 3:09 PM) (on file with author); *see Shadow 2 Forensics Tool in the Fight Against Child Exploitation*, PROSECURITY ZONE (Nov. 11, 2010), http://www.prosecurityzone.com/Customisation/News/Detection/Computer_Forensics_and_Data_Forensics/Shadow_2_Forensics_Tool_In_The_Fight_Against_Child_Exploitation.asp (explaining that the Shadow is compatible with all software programs); *What is the Shadow 2?*, *supra* note 286 (noting that the Shadow allows investigators to load forensics tools on the suspect’s computer).

The examiner would connect the Shadow and boot the suspect's computer with a boot CD or flash device and then hash the suspect's hard drive.²⁹² An examiner can also boot the suspect's computer with the Shadow, and load and run hashing programs.²⁹³ After the examiner finishes the hash analysis, the computer can then be taken off-site to be imaged and searched. The Shadow would allow on-site hash analyses to be conducted accurately and quickly, making the investigation much more similar to the drug dog sniff in *Caballes*.

In circumstances where police must perform imaging *and* hashing on-site,²⁹⁴ however, the suspect would be deprived of his computer for a considerable amount of time. As hard drive capacities have grown, with many holding at least a terabyte, it may take several hours to perform a KFF hash analysis of an entire drive.²⁹⁵ The time for hashing on top of imaging would deprive the suspect of his property for quite a while. While a dog's sniffing lasts a few moments, police would need access to the suspect's computer for hours in order to image it and conduct a hash analysis.

Courts are nevertheless sensitive to the time requirements of digital investigations. For example, in *United States v. Rubinstein*,²⁹⁶ the court held that it was reasonable for police to take four months to search the defendant's computer since other courts had also recognized the complexity involved in computer searches and, consequently, were lenient when delays occurred.²⁹⁷ Similarly, it took Huff two months to search Mann's computers and then another two months to search his external hard drive.²⁹⁸ In any event, police should have little trouble obtaining a warrant permitting seizure of the suspect's entire computer for off-site imaging since courts are typically lenient in permitting seizure of hardware for off-site review.²⁹⁹ If

²⁹¹ See *What is the Shadow 2?*, *supra* note 286.

²⁹² E-mail from David Biessener to Robyn Burrows, *supra* note 290.

²⁹³ *Id.*

²⁹⁴ For example, when police do not have warrant authorization to seize the digital evidence.

²⁹⁵ E-mail from Anthony V. Martino, Sergeant of the Utica, N.Y. Police Dep't, to Robyn Burrows (Oct. 13, 2010, 10:26 AM) (on file with author); Motto, *supra* note 85 (noting that it may take several hours to complete indexing); see also AccessData, Incident Response: Speed Can Mean the Difference Between Success and Failure, at 8, http://accessdata.com/downloads/media/IR_Speed_is_the_Difference.pdf (last visited Sept. 20, 2011) (displaying a "Pre-Process Timing Chart" indicating various times for indexing options). Performing a complete KFF analysis can be time consuming, even though the "computational process of hashing is lightning fast in execution." Losey, *supra* note 60, at 13.

²⁹⁶ No. 09-20611-CR, 2010 WL 2723186 (S.D. Fla. June 24, 2010), *report and recommendation adopted by* 2010 WL 2681364 (S.D. Fla. July 7, 2010).

²⁹⁷ *Id.* at *11-12 (citing, among other cases, *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (upholding a ten-month search)).

²⁹⁸ *United States v. Mann*, 592 F.3d 779, 781 (7th Cir.), *cert. denied*, 130 S. Ct. 3525 (2010).

²⁹⁹ See *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (holding that the government was permitted to remove the suspect's computer system because time, expertise, and a controlled environment were necessary); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (upholding seizure of computer equipment and its subsequent off-site search); *United States v. Lacy*, 119 F.3d 742, 746 (9th

all other options fail, police could always ask the suspect if he would allow them to image off-site and hash on-site.³⁰⁰

C. *Demonstrating Hashing in Court*

Even if case logs and on-site hashing are not persuasive enough for courts, police can always visually demonstrate their investigation. While juries may understand the gist of a forensic investigation, giving a visual demonstration can often be the key to establishing credibility over opposing counsel.³⁰¹ Unfortunately, many attorneys do not know how to properly present digital evidence.³⁰² Examiners are typically advised to use graphics during their testimony in order to support their opinion and convince both jurors and opposing counsel that the investigation followed proper protocol.³⁰³ In fact, “the single most important function of the expert is the development of graphics and exhibits for presentation of technical subjects to lay individuals.”³⁰⁴

Examiners may use large exhibit boards or computer graphics to display snapshots of their investigation.³⁰⁵ Even PowerPoint can be useful in giving the basics of what is “under the hood of a [PC].”³⁰⁶ An examiner can use graphics to explain the hardware and software as well as “the role the evidence has in relation to the case.”³⁰⁷ The best aids often contain a combination of audio and visual appeal.³⁰⁸ Using multimedia by combining “physical evidence, graphics, PowerPoint, and trial presentation technologies”

Cir. 1997) (permitting generic seizure of computer equipment because “a more precise description [was] not possible” since the government did not know where the images were located on the computer (quoting *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982)) (internal quotation marks omitted)); Joseph Audal et al., *Computer Crimes*, 45 AM. CRIM. L. REV. 233, 241 (2008) (noting that hard drives may be seized even if the warrant only mentions documents).

³⁰⁰ See *United States v. Simon*, No. 3:10-CR-56 RM, 2010 WL 4236833, at *1 (N.D. Ind. Oct. 20, 2010) (involving a situation where a suspect permitted examiners to remove some computers for off-site imaging because the examiners were having a difficult time imaging).

³⁰¹ PATRICK J. SULLIVAN ET AL., PRACTICAL ENVIRONMENTAL FORENSICS: PROCESS AND CASE HISTORIES 345 (2001) (“Most judges and juries have a gut understanding of technical issues. However, simple exhibits relating the issues to some ‘common experience’ can go a long way to clarifying and simplifying complex subjects.”). If using graphics during testimony, an examiner should provide a copy of the graphics to his attorney as well as opposing counsel. NELSON ET AL., *supra* note 45, at 553.

³⁰² Bruce A. Olson, *Engage the Jury: Presenting Electronic and Computer Forensics Evidence at Trial*, WIS. LAW., Feb. 2010, at 22, 22 (noting that many attorneys use too much jargon and make the expert’s testimony unintelligible or boring to the jury).

³⁰³ See NELSON ET AL., *supra* note 45, at 552-53.

³⁰⁴ SULLIVAN ET AL., *supra* note 301, at 345 (“Most assuredly, people (juries) react positively to a clear and well-demonstrated presentation that is both interesting and focused.”).

³⁰⁵ *Id.*

³⁰⁶ Olson, *supra* note 302, at 24.

³⁰⁷ NELSON ET AL., *supra* note 45, at 552-53.

³⁰⁸ *Id.* at 553.

creates a dynamic approach to digital evidence and allows the examiner to build a foundation upon which to describe technical details.³⁰⁹ The Shadow may also be a useful tool in giving the court a clearer picture of hashing since an examiner can hook up the Shadow to the suspect's computer and show the jury on a projector exactly how the examiner found the incriminating evidence.³¹⁰

Translating this to *Mann*, Huff could have visually demonstrated the entire hashing process to the court rather than merely describing how he imaged, hashed, and employed KFF to Mann's computers. Juries are more likely to understand a computer forensics investigation that is visually demonstrated.³¹¹ While it would seem like digital evidence would be especially incriminating to a defendant, the defense can easily attack its reliability and thwart a conviction since digital evidence is often complicated to explain to lay juries.³¹² Using strong visual aids prevents the defense from "pick[ing] apart the forensic reports and obfuscate[ing] facts by redirecting focus onto the computer forensic evidentiary process and interpretation."³¹³ Such visualization would also show judges that warrantless hash analyses are only revealing contraband and that weary courts, like the Ninth Circuit, need not be concerned about the government's "sophisticated hashing tools."³¹⁴

³⁰⁹ Olson, *supra* note 302, at 24. In addition, integrated evidence presentation systems ("IEPSs"), which "organize and present evidence of all types and forms," have been helpful in persuading juries. Elan E. Weinreb, Note, "Counselor, Proceed with Caution": *The Use of Integrated Evidence Presentation Systems and Computer-Generated Evidence in the Courtroom*, 23 CARDOZO L. REV. 393, 398 (2001).

³¹⁰ See Press Release, Voom Techs., Inc., *Battling Cybercrime: Criminals Can't Escape Their Own Digital Shadow When Investigators Use Voom's Computer Forensics Device* (Dec. 16, 2008), available at <http://www.reuters.com/article/idUS99300+16-Dec-2008+PRN20081216>. The Shadow was successfully used in the trial of Mark Jensen who was convicted in 2008 of murdering his wife by poisoning her with antifreeze. *Id.* Computer forensics analyst, Rhonda Mitchell, tried to explain how the chain of evidence was maintained during the investigation but the complicated technological processes were not easily translated to the jury. *Id.* Another examiner, Martin Koch, was then called to testify and subsequently used the Shadow to explain the evidence's reliability to the judge and jury. *Id.* Koch connected the Shadow to the suspect's computer and used a projector to show the courtroom multiple Internet websites Mark Jensen had accessed, including websites explaining antifreeze poisoning. *Id.* The jury noted that evidence displayed via the Shadow was essential in reaching its guilty verdict. *Id.*

³¹¹ Weinreb, *supra* note 309, at 395; see also Press Release, Voom Techs., Inc., *Minnesota High-Tech Company Helps Detectives and Prosecutors Fight Crime and Terrorism*, at 1 (May 26, 2008), available at <http://www.voomtech.com/downloads/Shadow2/newsrelease.pdf> ("[W]ithout the Shadow, the jury is never quite sure if an evidentiary report reasonably reflects what the defendant was up to." (emphasis omitted)).

³¹² FERRARO ET AL., *supra* note 21, at 278.

³¹³ Press Release, *supra* note 311, at 1 (emphasis omitted). Essentially, the "computer becom[es] a witness." Weinreb, *supra* note 309, at 404.

³¹⁴ *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 999 (9th Cir. 2009), *superseded by* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam).

CONCLUSION

In the future, judges will likely be more comfortable with technology and perhaps more eager to allow investigators warrantless use of tools like KFF. Computer forensics is still a relatively new field and until a computer savvy generation sits behind the bench, judges will likely need an assurance that technology is not being used to cut corners. The principles of *Caballes* certainly apply to hash analyses, yet the “digital drug dog sniff” context is novel enough to require a temporary compromise. Case logs may help courts feel more comfortable with warrantless hashing since they represent a level of accountability. Further, conducting the hash analysis on-site will create a context more similar to *Caballes* and one that will likely be more attractive to judges. Lastly, prosecutors would be wise to demonstrate KFF in court so that judges and juries can get a visual of the software. While courts need to be better educated as to the particulars of hash analyses, there is still merit in adopting temporary compromises that allow courts to gradually apply Fourth Amendment law to the complex field of computer forensics.