Volume VII - Article 5

COMPUTER FORENSICS, SEARCH STRATEGIES, AND THE PARTICULARITY REQUIREMENT

Wayne Jekot[†]

Spring 2007

Abstract

Assuming that a person subject to a search and seizure of his or her computer has a reasonable expectation of privacy in the contents of the computer, and thus a warrant is required, should the warrant outline a "search strategy"? Or should comprehensive computer searches be permitted? In other words, how should the particularity requirement be applied to computer searches? Correspondingly, what can a forensic examiner do under a warrant while collecting potential evidence from a computer?

Current computer forensic methodology calls for seizing the entire computer, making a mirror image of the hard drive, and then forensically examining the contents of the drive off-site. While examining the contents of the drive, all user (i.e., non-system) files must be inspected, regardless of their file extensions and potential relevance to the case.

There are various justifications for this methodology. First, it is accepted that the computer must be seized and examined off-site because the forensic examinations of the sizable hard drives of today take too long on-site and require specialized computer equipment. Accepted practice also requires that the forensic examiner make a mirror image of the hard drive to avoid changing the contents of the original hard drive. In addition, the forensic examiner must look at every user file because file extensions can be misleading and relevant evidence could be found even in files that are seemingly unrelated to the current investigation. If the examiner finds of evidence of, for example, child pornography while searching for evidence of fraud, the examiner must then get

---

[†] Juris Doctor, University of Connecticut School of Law, 2006. The author would like to thank the Honorable Michael R. Sheldon, the Honorable John F. Blawie and Dr. Al Harper for their comments, suggestions and support.

a second warrant to continue to search for more child pornography.

Thus, a warrant not only permits a search, it also serves to limit that search. The Fourth Amendment requires that warrants "shall issue particularly describing the place to be searched and the person or things to be seized." This is accomplished through the particularity requirement: a warrant must be sufficiently precise so that the officer executing the warrant can with reasonable effort ascertain and identify the place intended. Furthermore, the description must leave nothing to the discretion of the officers. There are exceptions, such as good faith and plain view, but the officer cannot search in a "breadbox for an elephant."

In the physical world, those standards are easily applied. A warrant is issued describing in detail the place to be searched. For instance, a search warrant may authorize a police officer to search for controlled substances in a person's home at a certain time. An officer may not seize the entire contents of the home, carry them away and then search them at his leisure. His search is limited by the contents of the warrant.

In the computer context, however, the particularity requirement has seemingly been abandoned. Search warrants for computers could be likened to the "Writs of Assistance" that the particularity requirement of the Fourth Amendment was intended to eliminate. Under current practice, computers, which can store the same amount of data found in a full library, are seized, taken off site and then rummaged through by a forensic examiner. On-site searches for particular computer files are too "difficult" and "time consuming." The needs of law enforcement – and not Fourth Amendment rights – control the content of warrants.

This state of affairs has been accepted (or at least tolerated) because computer searches are seen as "special." The computer world is unlike the physical one. As a result, courts have struggled to apply Fourth Amendment law that was developed from cases in the physical world (e.g., what is "plain view" in cyberspace?). One solution is to create new Fourth Amendment rules for computer searches. Alternatively, law enforcement could use methods that comport with the Fourth Amendment. Perhaps the details of the accepted trilogy of acquisition, authentication and analysis can be reworked as new technologies become available.

This paper will discuss computer forensics, search strategies and the particularity requirement. Part II will be an overview of computer technology. Part III will examine accepted computer forensic methodologies and principles and their justifications. Part IV will discuss the Fourth Amendment, warrants and the particularity requirement in the context of computer searches. Analogous physical world searches will be discussed. Part V will outline alternative methods for the forensic examination of computers. In addition to the accepted practice of off-site comprehensive computer searches, various methods, tools and technology are, or could be, available to computer forensic examiners. Instead of adapting warrants to the needs of law enforcement, perhaps those alternatives will allow law enforcement to undertake computer searches, while still preserving Fourth Amendment rights.

TABLE OF CONTENTS

[1] *See* CRIMINAL JUSTICE TECHNOLOGY IN THE 21ST CENTURY *passim* (Laura J. Moriarty & David J. Carter, eds., 2005) [hereinafter "CRIMINAL JUSTICE"] (noting the increase in computer-based and computer-related crimes in the past few decades).

I. INTRODUCTION

Criminal investigations increasingly involve evidence from personal computers. [1] Searching and seizing personal computers present problems that traditional, physical world searches do not.[2] Unlike in the physical world, where an officer can go to a physical location, search for a tangible item, and then possibly seize it, law enforcement is faced with many variables when searching computers. Computer data is fragile and easily destroyed. The amount of data found on a computer is complex and voluminous. Computer files may have misleading names or may be hidden.

As a result, warrants to search computers have difficulty "particularly describing the place to be searched, and the persons or things to be seized."[3] The particularity requirement prevents law enforcement from executing "general warrants" that permit "exploratory rummaging" through a person's belongings in search of evidence of a crime.[4] But the complexity of computers makes it difficult for law enforcement to determine beforehand what hardware should be seized and what files should be searched. The solution frequently comes in the form of a "search strategy": the affidavit lists the specific hardware to be seized and searched and explains the techniques that will be used to search only for the specific files related to the investigation, and not every file on the computer.[5]

When searching the computer, a forensic examiner uses the search strategy as a guide. Even so, a forensic examiner will often search files that are unrelated to the investigation. For example, if the search strategy allows the examiner to look for files containing the word "drug",

---

[2] U.S. DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS pt. II.A (2002), http://www.cybercrime.gov/s&smanual2002.htm [hereinafter "SEARCHING AND SEIZING"].
[3] U.S. CONST. amend. IV.
[4] Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).
[5] SEARCHING AND SEIZING, *supra* note 2, pt. II.C.3.

the examiner may find files related to legal prescription drugs – not just controlled substances. Furthermore, the forensic examiner may find evidence of other crimes besides the one under investigation. For example, the examiner may be searching for evidence of fraud, and while doing so, find images of child pornography. Thus, the search of a computer is not only controlled by the warrant, but also by other practical and technical considerations.

This paper will discuss computer forensics, search strategies and the particularity requirement of the Fourth Amendment. Assuming that a person who is subjected to the search and seizure of his or her computer has a reasonable expectation of privacy in the contents of the computer, and thus a warrant is required, what type of "search strategy" should the warrant outline? How comprehensive should a computer search be? In other words, how should the particularity requirement be applied to computer searches? Correspondingly, what should a warrant authorize a forensic examiner to do while collecting potential evidence from a computer?

Part II will be an overview of relevant computer technology. Computer technology encompasses many devices, but this part will focus on the personal computer. Part III will discuss accepted computer forensic methodologies and principles and their justifications. Part IV will discuss the Fourth Amendment, warrants, and the particularity requirement in the context of computer searches. Analogous physical world searches will also be discussed. Part V will outline alternative methods for the forensic examination of computers. This part will also critically examine the justifications for accepted computer forensic methodologies and principles. In addition to accepted computer forensic practices, various methods, tools and technology are, or could be, available to computer forensic examiners.

II. OVERVIEW OF RELEVANT COMPUTER TECHNOLOGY

a. Architecture

Digital evidence can come from a variety of sources, such as computer programs, computer networks and other electronic devices such as cell phones, beepers and personal digital assistants.[6] Although there are many possible sources of digital evidence, the most common type of digital evidence used in criminal courts is from personal computers ("PC"s).[7]

PCs are composed of many parts, including input and output devices, memory, storage devices, central processing units ("CPU"s) and data buses.[8] Examples of input devices are mice and keyboards.[9] Monitors and printers are output devices.[10] Memory is where programs and data are stored temporarily while the PC is turned on.[11] There are many types of memory within a computer, including cache and flash memory, but the most familiar type is Random Access Memory ("RAM").[12] Storage devices are where programs and data are stored permanently.[13] Hard disks, floppy disks, CDs and DVDs are examples of storage devices.[14] The data on storage devices is relatively static compared to the data that passes through memory.[15] The CPU is the "brain" of the computer: it executes programs stored in memory by fetching, examining and executing instructions.[16] Finally, the data bus is a set of wires that connects all the computer parts and transmits data from one part to another.[17]

---

[6] EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS, AND THE INTERNET 12-13 (2d ed. 2004).
[7] S*ee* ROBERT W. TAYLOR ET AL., DIGITAL CRIME AND DIGITAL TERRORISM 305 (2006) (noting that storage devices, which are a part of PCs, are the primary source of evidence in criminal courts).
[8] *See generally* ANDREW S. TANENBAUM, STRUCTURED COMPUTER ORGANIZATION 39-116 (4th ed. 1999) (describing how computers are organized).
[9] *Id.* at 92-93, 99-101.
[10] *Id.* at 93-99, 101-06.
[11] *Id.* at 56.
[12] *Id.* at 152.
[13] *Id.* at 69.
[14] TANENBAUM, *supra* note 8, at 69.
[15] TAYLOR ET AL., *supra* note 7, at 305.
[16] TANNEBAUM, *supra* note 8, at 39.
[17] *Id.*

The forensic examination of a computer centers on storage devices, because storage devices retain data even when the computer is turned off.[18] The data in other parts of the computer is lost when the computer is powered off.[19] Of the various types of storage devices, hard drives are usually the richest source of data from computers.[20] There are a number of different hard drive technologies, such as Integrated Drive Electronics ("IDE") and Small Computer System Interface ("SCSI"), but all have a disk controller, which is a computer chip that controls the drive.[21] Also, regardless of type, hard drives contain one or more platters with a magnetic coating.[22] If there is more than one platter, the platters are stacked vertically.[23] Each platter spins under a disk head, which floats over the platter and reads and writes data to it.[24]

To write to the platter, negative and positive current is passed through the disk head, which then magnetizes the platter that is spinning underneath it.[25] To read from the platter, the positive or negative current from the disk is induced in the disk head.[26] Each positive or negative impulse represents a bit.[27] The bit is the smallest storage unit in a computer.[28]

b. Computer Data

A bit may contain a one or a zero.[29] Eight bits make a byte.[30] Although stored on hard

---

[18] There are ways to collect evidence from other parts of the computer when the computer is turned on. For instance, a forensic examiner can take pictures of the monitor.
[19] One exception is the Complementary Metal Oxide Silicon ("CMOS") chip found in PCs: a battery allows this chip to store computer configuration details, such as the system date, time, and hard drive parameters, even when the computer is turned off. CASEY, *supra* note 6, at 196.
[20] *Id.* at 200.
[21] TANENBAUM, *supra* note 8, at 73. "SCSI" is pronounced "scuzzy." SCOTT MUELLER, UPGRADING AND REPAIRING PCS 514 (13th ed. 2001).
[22] *Id.* at 70.
[23] *Id.* at 71.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] TANENBAUM, *supra* note 8, at 71.
[28] *Id.* at 56.
[29] *Id.*
[30] *Id.* at 58.

drives as bytes, computer data is manipulated and transmitted by a computer in the form of serial bit streams.[31] A serial bit stream is a string of bits (e.g., 00011001). The conversion from bytes to a serial bit stream and vice versa is done by the hard drive controller.[32]

Appended to the end of a serial bit stream is an error correcting code ("ECC").[33] An ECC is used to verify that the serial bit stream has not been corrupted by, for instance, a voltage spike.[34] An ECC is calculated using one of any number of algorithms.[35] The algorithm uses the ones and zeroes in the data bits to compute the ECC's value.[36] That computation can then be done again later.[37] The computed ECC can then be compared to the stored ECC to verify the integrity of the data.[38] Various parts of the computer, including the hard drive controller, can compute an ECC.[39]

Computer users do not see bits, bytes, strings of ones and zeros or ECCs. Computer users see files. The operating system –for instance, Windows XP – organizes the underlying ones and zeroes into the files and folders that are familiar to computer users through a graphic user interface. Many of the files found on computers are a part of the operating system, and thus much of the data found on hard drives is a part of the operating system.[40]

c. File Systems

The operating system determines how files are organized. Each operating system has its own way of organizing files, and the particular type of organization is known as the file system.

---

[31] *Id.* at 73
[32] *Id.*
[33] TANENBAUM, *supra* note 8, at 61.
[34] *Id.*
[35] *Id.* at 61-64.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] TANENBAUM, *supra* note 8, at 73.
[40] CASEY, *supra* note 6, at 229-30.

For example, Windows XP uses the NT File System ("NTFS"), Macintosh uses the Macintosh Hierarchical Filesystem ("HFS"), and UNIX uses various file systems, including the UNIX File System ("UFS").[41] The file system keeps track of where data is located on a hard drive.[42] It does so through a system-created file known as the file allocation table ("FAT").[43] The FAT could be likened to a library card catalog: just as a card catalog tells a person where to find a book in the library, the FAT tells the operating system where to find a file. When a file is deleted, the FAT entry is deleted, but the underlying data is left on the hard drive until it is overwritten by other data. In other words, hitting the "delete" key, without more, will merely change the status of the file in the FAT. This is analogous to someone removing a card from the card catalog but leaving the book on the shelf: the book could still be found but not by looking in the card catalog.[44]

The file system also controls file extensions. File extensions, such as "doc", "jpg", and "htm", are one to three character identifiers that appear after the file name.[45] File extensions inform the user and the operating system of the file's type. The file extension can be changed by a user, without changing the actual type of file.[46] For instance, "doc" can be changed to "jpg", but the file will still be a Microsoft Word document and not an image document, because the file itself contains an internal header that specifies the file type.[47]

III. ACCEPTED COMPUTER FORENSIC PRINCIPLES AND METHODOLOGIES AND THEIR JUSTIFICATIONS

The field of computer forensics covers the principles and methodologies used to collect,

---

[41] *Id.* at 202, 291.
[42] *Id.*
[43] MUELLER, *supra* note 21, at 1316-17. Here "FAT" is used generically: each operating system has its own name for the FAT, but the underlying principle is the same.
[44] CASEY, *supra* note 6, at 203.
[45] MUELLER, *supra* note 21, at 1382.
[46] *See* CASEY, *supra* note 6, at 230-31.
[47] *Id.* at 230.

preserve and examine evidence from computers.[48] Most often this evidence comes from a storage device, such as a hard drive, because the data found on a storage device is relatively static compared to the volatile data that passes through the other parts of a PC.[49] The established methodologies used to obtain evidence from storage devices fall into three broad stages: acquisition, authentication and analysis.[50]

a. Acquisition

Assuming there is legal authority for the search,[51] the forensic examiner must first prepare by having the proper equipment, such as computers and software used to acquire data, in place.[52] The forensic examiner must also be prepared to document all aspects of the search: who collected the evidence, when it was collected, from where it was collected and how it was collected.[53]

After those preliminaries, the forensic examiner must acquire the potential computer evidence. At this stage, there are four possible ways to do so: (1) search the computer and print hard copies of particular files on-site; (2) search the computer and make an electronic copy of particular files on-site; (3) create a duplicate electronic copy of the entire storage device on-site for later off-site examination; or (4) seize the computer hardware, remove it from the premises

---

[48] *See* ROBERT M. SLADE, SOFTWARE FORENSICS: COLLECTING EVIDENCE FROM THE SCENE OF A DIGITAL CRIME 2-4 (2004) (discussing the difference between digital forensics, which covers all digital devices, and computer forensics, which is concerned with computer storage devices).

[49] TAYLOR ET AL., *supra* note 7, at 305.

[50] *Id.* at 307-319; CASEY, *supra* note 6, at 212-51; U.S. DEPT. OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 1-2 (2004), *available at* http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm (last visited Oct. 10, 2005) [hereinafter "FORENSIC EXAMINATION"].

[51] Various legal issues related to searching computers will be discussed *infra* in part IV.

[52] CASEY, *supra* note 6, at 215. The computers should not be connected to a public network, such as the internet, because there is a risk of unauthorized access. *Id.* at 227.

[53] *Id.* at 218.

and review its contents off-site.[54]

Each method has its own advantages and disadvantages. Printing hard copies of particular files on-site is quick and simple.[55] Even a police officer with limited computer knowledge can do it. Printing is also the least disruptive method.[56] If the PC is part of a private computer network or is needed to conduct legitimate business purposes, printing will not disturb those activities. Moreover, if part of a private network, the system administrator or owner may be able to assist in the collection of data from the PC.[57]

But simply printing files may cause "substantial loss of information, including file date and time stamps, file path name, 'undo' history, comment fields and more."[58] This information is known as metadata.[59] Metadata is data about the data and is either stored internally within a file or in other operating system files.[60] Metadata can yield relevant evidence. For example, it can be used to determine who created a file and when and where the user did so.[61] If an officer simply prints a file, the metadata associated with that file will not be examined.

The second method of acquiring computer data – searching a computer on-site and making electronic copies of particular files – captures the metadata that is stored internally within files. Like printing, this method is simple and causes minimal disruption.[62] However, this method is disfavored because, by only copying some files and not all of them, potential evidence may be overlooked or may not be readily apparent to the examiner on-site.[63] Furthermore, there

---

[54] SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.
[55] CASEY, *supra* note 6, at 225, 228.
[56] *Id.*
[57] *Id.*
[58] SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.
[59] CASEY, *supra* note 6, at 273.
[60] HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY 134, 147, 189 (Eoghan Casey ed., 2004) [hereinafter "HANDBOOK"].
[61] *Id.* at 189.
[62] CASEY, *supra* note 6, at 228.
[63] *Id.* at 225, 228.

is a risk that the "system has been modified to conceal or destroy evidence,"[64] and potential evidence is not readily apparent to the examiner. In addition, on-site searches are time-consuming: "[g]iven that personal computers sold in the year 2002 usually can store the equivalent of thirty million pages of information and networks can store hundreds of times that (and these capacities double nearly every year), it may be practically impossible for agents to search quickly through a computer for specific data, a particular file or a broad set of files while on-site."[65] Finally, in copying (or printing) individual files on-site, data may be unintentionally altered or destroyed.[66] Such actions may change, for instance, the time-date stamp that indicates when a file was last accessed. Also, just turning on a PC may change files. For example, during the start-up process of the Windows NT operating system, five hundred files are altered.[67]

The third method of acquiring data, creating a duplicate electronic copy of the entire storage device on-site for off-site examination, overcomes some of the limitations of the first two methods. Copying an entire storage device prevents changes or damage to the original.[68] Also, taking the copy off-site allows for painstaking examination in a controlled environment.[69] Moreover, all data is copied, including metadata, system-created files, and deleted files. "Given the risks in collecting only a few files, in most cases, it is advisable to acquire the full contents of the disk because digital investigators rarely know exactly what a disk contains."[70]

All data on a storage device is captured through a procedure known as disk imaging.[71] Disk imaging uses software programs to copy a storage device at the bit level, and each bit on

---

[64] *Id.* at 225.
[65] SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.b.
[66] CASEY, *supra* note 6, at 228.
[67] TAYLOR ET AL., *supra* note 7, at 308.
[68] CASEY, *supra* note 6, at 228.
[69] *Id.*; *see also* SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.b (arguing that "[r]ecovering the evidence may require painstaking analysis by an expert in the controlled environment of a forensics laboratory").
[70] CASEY, *supra* note 6, at 226.
[71] TAYLOR ET AL., *supra* note 7, at 309. Disk imaging is also known as disk mirroring. *Id.*

the original is reproduced in the copy.[72] The resulting "image" of the original is known as a bit stream copy.[73] A bit stream copy is an exact duplicate of the original storage device.[74] This differs from a logical copy, in which a copy is made of the files that are accessible to a user through the operating system.[75]

An example helps to illustrate the difference. Consider a file on a hard drive. Because of the manner in which data is written to the hard drive, rarely will one file be stored intact in one place on a hard drive. The file is usually broken into parts, and each part may be on a different part of the hard drive. This is known as file fragmentation.[76] Together, the parts form the single file that a user sees on screen through the operating system. At the lowest level, the individual parts of the file are comprised of bits.[77] Because a file is often fragmented, the bits may be on different parts of the drive. When a logical copy is made, the structure of files and folders as viewed through the operating system is copied, but the underlying parts may be copied to different locations and in a different order. Thus, the organization of the bits on the copy may be different from the original. However, a bit stream copy reproduces the storage device at the bit level. The underlying structure and order of bits is copied exactly from the original to the reproduction.

Because disk imaging copies all bits, the bit stream copy contains all data on the hard drive – including deleted data. A logical copy will not reproduce deleted files, because the deleted files are not accessible to the operating system.[78] The operating system is cognizant of

---

[72] *Id.* (leaving the original data *in situ* and intact on the original drive).
[73] *Id.*
[74] CASEY, *supra* note 6, at 226. When an original hard drive is replaced with a hard drive containing a bit stream copy of the original, the change is transparent to any user, unless he or she opens the computer and looks at the hard drive and finds a difference in serial number or make and model.
[75] CRIMINAL JUSTICE, *supra* note 1, at 249.
[76] *See* CASEY, *supra* note 6, at 265.
[77] *See supra* Part II.b.
[78] TAYLOR ET AL., *supra* note 7, at 310.

only the files found in the FAT.[79] If a file has been deleted, it is no longer listed in the FAT, although the underlying data may still be stored on the hard drive.[80] Disk imaging captures the underlying data because it does not rely on the FAT in making a copy.

In addition to disk imaging, the third method of acquiring data employs read-only tools called write-blockers.[81] Write-blockers are either hardware devices or software programs that prevent any data from being added, deleted or altered on the original storage device.[82] Write-blockers are found to be necessary because a "major aspect of preserving digital evidence is collecting it in a way that does not alter it."[83]

Although the third method has advantages over the first two, it is deprecated because imaging a storage device on-site may be time consuming.[84] More importantly, the original evidence is left behind when the examiner takes the copy off-site for examination: "[f]ield acquisition is not the preferred method, because failure to maintain control of the evidence drive can also lead to problems in establishing the authenticity of the evidence in court."[85] One way around this difficulty is to make a mirror image of the hard drive, replace the original with the mirror image, and then take the original off-site.

However, the universally accepted solution to those limitations is the fourth method of data acquisition: seizing all computer hardware, removing it from the premises and reviewing its contents off-site.[86] This method makes the hardware available for others to examine at a later

---

[79] *See supra* Part II.c.
[80] *See supra* Part II.c.
[81] CRIMINAL JUSTICE, *supra* note 1, at 249 Write-blocking is also sometimes referred to as write-protection.
[82] *Id.*
[83] CASEY, *supra* note 6, at 220.
[84] *Id.*; *see also* SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.b. (arguing that "[a]gents cannot reasonably be expected to spend more than a few hours searching for materials on-site").
[85] TAYLOR ET AL., *supra* note 7, at 307.
[86] *See generally* CYBERCRIME: THE INVESTIGATION, PROSECUTION, AND DEFENSE OF COMPUTER-RELATED CRIME 83 (Ralph D. Clifford ed., Carolina Academic Press 2001) (noting that the off-site search of a computer is an "accepted practice") [hereinafter "CYBERCRIME"].

date.[87] Further, the actual collection of the hardware, known colloquially as "tagging and bagging", takes little technical expertise.[88] And like the third method, the hardware can later be examined in a controlled environment.[89]

The off-site examination of hardware shares other similarities with the third method. The term "hardware" encompasses the physical components of the PC – individually and as a whole. Thus, a hard drive is a piece of hardware. Consequently, an off-site examination of PC hardware employs both disk imaging and write-blocking.[90] Because of its similarities to the third method, the fourth method also overcomes the difficulties of the first two methods of data acquisition. For example, all data, including metadata and deleted files, may be examined.

All authorities agree that the fourth method is a "best practice" and is preferred over the other three.[91] In essence, this amounts to taking the entire PC off-site, making a bit stream copy of the hard drive and then forensically examining the contents of the copy.

b. Authentication

After the hardware has been acquired, but before the data on the storage device can be analyzed, the data must be authenticated.[92] Authentication involves comparing the original data to the copy and verifying that the two are the same.[93]

Data is authenticated through software that uses a hashing algorithm.[94] A hashing algorithm takes a set of data as input and produces a distinct numerical output known as a hash

---

[87] CASEY, *supra* note 6, at 228.
[88] *Id.*
[89] *Id.*
[90] *Id.* at 226 (stating multiple bit stream copies of a hard drive may be made for backup purposes).
[91] TAYLOR ET AL., *supra* note 7, at 305, 319; CASEY, *supra* note 6, at 226; CRIMINAL JUSTICE, *supra* note 1, at 249; SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.
[92] TAYLOR ET AL., *supra* note 7, at 308 (stating that while related, this form of authentication is not to be confused with the evidentiary foundation requirement of authentication).
[93] CASEY, *supra* note 6, at 219.
[94] TAYLOR ET AL., *supra* note 7, at 308; CASEY, *supra* note 6, at 218-19. Hashing algorithms are also known as message digest algorithms.

value.[95] Hash values are analogized to fingerprints, because the probability of any two different sets of data having the same hash value is extremely low.[96] Different data sets produce different hash values, even if the data differs by only one bit,[97] but an exact copy will have the same hash value as the original.[98]

A hash algorithm is a mathematical function. A mathematical function takes a value as an input and produces a unique output value.[99] The formal definition of a function is: "[a] function *f* is a rule that assigns to each element *x* in a set *A* exactly one element, called *f(x)*, in a set *B*."[100] In general, a function is represented by $y = f(x)$, where y is the output, x is the input, and f is the function.[101] For example, $y = f(x) = x + 1$ is a function. When $x = 2$, f takes 2 as an input and the value of the output y is $3 = f(2) = 2 + 1$. It is helpful to think of a function as a machine that implements a rule: when a value is input to the machine, the machine outputs a value according to a rule.[102] In the above example, the rule is "add 1 to whatever number is input."

Similarly, a hash algorithm is a function that takes a value as an input and produces a unique output value.[103] The inputs are computer data and the outputs are unique numerical values.[104] The function itself is implemented through computer code within a computer program.[105] There are a number of hashing algorithms in use today, such as: Message Digest

---

[95] TAYLOR ET AL., *supra* note 7, at 308 (stating thus, a hash value is similar to an ECC). *See supra* Part II.b.
[96] For one algorithm, the probability of having two sets of data with the same hash value has been calculated as either 1 in 2^{28} , CASEY, *supra* note 6, at 219, or 1 in 10^{37}, TAYLOR ET AL., *supra* note 7, at 309. For the same algorithm, the probability of creating a set of data with a given hash value is 1 in 2^{128}. CASEY, *supra* note 6, at 219; HANDBOOK, *supra* note 60, at 117 n.1.
[97] CASEY, *supra* note 6, at 219-20.
[98] *Id.* at 219.
[99] KENNETH H. ROSEN, DISCRETE MATHEMATICS AND ITS APPLICATIONS 57 (4th ed. 1999).
[100] JAMES STEWART, CALCULUS: CONCEPTS AND CONTEXTS, SINGLE VARIABLE 12 (1998).
[101] GEORGE F. SIMMONS, PRECALCULUS MATHEMATICS IN A NUTSHELL: GEOMETRY, ALGEBRA, AND TRIGONOMETRY 51 (Barnes & Noble Books, 1997).
[102] STEWART, *supra* note 100, at 13.
[103] TAYLOR ET AL., *supra* note 7, at 308-09.
[104] *Id.*
[105] *Id.*

Algorithm 5 ("MD5"), Secure Hash Algorithm ("SHA"), HAVAL and SNEFRU.[106] The most commonly used algorithms are MD5 and SHA.[107] Each algorithm uses a different set of rules to produce a unique output value for a given input.[108]

Although computer users see images, words and decimal numbers on a computer screen through the graphic user interface, on an electronic level computers manipulate and store such data in the form of serial bit streams (e.g., 10011001).[109] Thus, hash algorithm input values are in the form of serial bit streams. Output values are in the hexadecimal numerical format, whereby eight binary characters are represented by a combination of two hexadecimal characters.[110] Hexadecimal is a base-sixteen number system and uses the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F.[111] For example, 3C is a hexadecimal number and it is equal to 00111100 binary and 60 decimal.[112]

The previous example shows how a decimal number is represented in binary and in hex. A hashing algorithm does not simply convert from one number system to another however. A hashing algorithm implements a rule that computes a unique hex value for a given string of bits. For instance, when the text sentence 'The quick brown fox jumps over the lazy dog' is input into the MD5 hashing algorithm, the result is the thirty-two digit hexadecimal number '9E 10 7D 9D

---

[106] CASEY, *supra* note 6, at 219.
[107] *Id.* ("SHA is very similar to MD5 and is currently the U.S. government's message digest algorithm of choice.").
[108] The rules are complicated and beyond the scope of this paper.
[109] *See supra* Part II.b.
[110] *Id.*
[111] TANENBAUM, *supra* note 8, at 634.
[112] *Id.* at 635. Consider another example, one that involves text. The sentence 'The quick brown fox jumps over the lazy dog.' contains forty-four characters, including the spaces and period, and can represented by forty-four bytes (or three hundred fifty-two bits, with eight bits to a byte) as: '01010100 01101000 01100101 00100000 01110001 01110101 01101001 01100011 01101011 00100000 01100010 01110010 01101111 01110111 01101110 00100000 01100110 01101111 01111000 00100000 01101010 01110101 01101101 01110000 01110011 00100000 01101111 01110110 01100101 01110010 00100000 01110100 01101000 01100101 00100000 01101100 01100001 01111010 01111001 00100000 01100100 01101111 01100111 00101110' (the spaces between the bytes are added to facilitate reading). The forty-four bytes can be represented by forty-four hexadecimal numbers: '54 68 65 20 71 75 69 63 6B 20 62 72 6F 77 6E 20 66 6F 78 20 6A 75 6D 70 73 20 6F 76 65 72 20 74 68 65 20 6C 61 7A 79 20 64 6F 67 2E' (the spaces between the hex numbers are added to facilitate reading).

37 2B B6 82 6B D8 1D 35 42 A4 19 D6'.[113] In mathematical notation, that example becomes:

> $f(x) = y$ = MD5(The quick brown fox jumps over the lazy dog) = 9E107D9D372BB6826BD81D3542A419D6, where f = MD5, x = The quick brown fox jumps over the lazy dog, and y = 9E107D9D372BB6826BD81D3542A419D6.
>
> If the input is changed by one character, the output is completely different:
> MD5(The quick brown fox jumps over the lazy dogs) = 3EE6F92B7CDDC3F50B7D 2DDD145B018B.
>
> And if a different hashing algorithm is used, SHA-1 (a version of SHA), the output is a forty-digit hexadecimal number:
> SHA-1(The quick brown fox jumps over the lazy dog) = 2FD4E1C67A2D28FCED84 9EE1BB76E7391B93EB12.

The examples show a sample text string and an actual hash value for that string. However, a hashing algorithm is used in computer forensics to compute the hash value for a much larger set of input data – generally the entire set of bits found on a hard drive.

Hashing algorithms and hash values are used at various stages of the forensic examination of data. First, before anything else is done with the original hard drive, the hash value of its data is calculated.[114] Also, a hash value for the analysis disk – the hard disk to which the original will be copied – is calculated.[115] After copying the original hard drive to the analysis disk, the hash value of the analysis disk then should be calculated.[116] The hash values of the original and of the copy are then compared. If they match, then the analysis drive is a "true and authentic copy of the original evidence."[117]

The hash values of individual files can also be calculated. Instead of inputting all bits on

---

[113] A variety of computer programs available on the internet implement hashing algorithms.
[114] TAYLOR ET AL., *supra* note 7, at 308; CASEY, *supra* note 6, at 219.
[115] TAYLOR ET AL., *supra* note 7, at 311. The analysis disk should be completely blank. If an analysis disk is reused, its hash value should match the hash taken when the drive was new and empty. The accepted practice to erase the contents of an analysis drive is the "DoD wipe": this is a standard set by the U.S. Dept. of Defense to sanitize hard drives that contain data that is not classified as top secret. *Id.* at 311, 327.
[116] *Id.* at 308, 310; CASEY, *supra* note 6, at 219.
[117] TAYLOR ET AL., *supra* note 7, at 308.

the hard drive, only the bits associated with an individual file are input to a hash algorithm. This can be used to verify that an individual file has not changed. This can also be used to match identical files – even if the files have different names.[118] In addition, a forensic examiner can use hash values to sort unknown files from common software programs and system files.[119] Individual file hashing is also used by the FBI's "Innocent Images National Initiative," which compares the hash values of evidence files with those of known child pornographic images.[120]

Although hash values are touted as "unique"[121] and have been compared to "fingerprints,"[122] researchers have created different data sets with identical MD5 and SHA hash values.[123] When a hash algorithm produces the same hash value for two different data sets, the result is known as a collision.[124] Researchers have found MD5 collisions in fifteen minutes on a simple laptop computer.[125] Even so, MD5 and SHA continue to be used, but in time they will likely be replaced by more robust hashing algorithms.[126]

Hashing algorithms are employed because they help to establish that the evidence ultimately used in court is reliable.[127] Hash values are used to demonstrate that the results of the forensic analysis are an authentic product of the evidence seized.[128] However, a hash value alone

---

[118] CASEY, *supra* note 6, at 220.
[119] Paul L. Luehr, Real Evidence, Virtual Crimes: The Role of Computer Forensic Experts, 20 CRIMINAL JUSTICE 14, 17 n. 3 (2005).
[120] Shawne K. Wickham, *High-tech Tools Track Porn Traffickers*, N.H. UNION NEWS, May 8, 2005, at A17. As of May 2005, the FBI has stored more than thirty thousand hash values of child pornographic images, and the Customs Service has stored ninety thousand such values. *Id.*
[121] TAYLOR ET AL., *supra* note 7, at 308.
[122] CASEY, *supra* note 6, at 219.
[123] Rick Merritt, *Crack in SHA-1 Code 'Stuns' Security Gurus*, E.E. TIMES, Feb. 21, 2005, at 1; Kevin Murphy, *Crypto Scrutinized After Hash Flaws Found*, COMPUTERGRAM (COMPUTERWIRE), Aug. 19, 2004.
[124] Roger Howorth, *Hash Research Blow to Security*, IT WEEK, June 1, 2005, http://www.itweek.co.uk/itweek/news/2137376/hash-research-blow-security (last visited Mar. 27, 2007). In mathematics, a function for which each output has exactly one input is said to have a one-to-one correspondence. ROSEN, *supra* note 99, at 59. Hash algorithms are intended to be one-to-one but are not if a collision is found.
[125] Howorth, *supra* note 124.
[126] Luehr, *supra* note 119, at 18.
[127] CASEY, *supra* note 6, at 220.
[128] *See* TAYLOR ET AL., *supra* note 7, at 308-09.

does not demonstrate that the evidence is reliable, because data could be altered before a hash value has been calculated.[129] As with other types of evidence, "the trustworthiness of digital evidence comes down to the trustworthiness of the individual who collected it."[130] Even if a hashing algorithm is used, the proponent must prove that the evidence presented in court is unaltered.

c. Analysis

Once the hardware has been acquired and the data has been authenticated, the next stage in the forensic examination of a PC is to analyze the data. The analysis is done using a copy of the data and not the original data and storage device.[131] The "analysis should preserve the integrity of the digital evidence and should be repeatable and free from distortion or bias."[132]

The first step in the analysis stage is typically data reduction.[133] This is necessary because today's hard drives can contain a large volume of data. For instance, a forty gigabyte hard drive can contain the equivalent of twenty million typewritten pages.[134] Much of the data on a hard drive is part of the operating system or of known computer programs.[135] A forensic examiner can filter out such data using file hashing: the hash values of files on the evidence drive are compared with known hash values and matching files are not analyzed.[136]

After the data reduction step, the nature and extent of analyses of storage devices vary greatly, depending on the crime under investigation.[137] By first determining the types of digital

---

[129] CASEY, *supra* note 6, at 220.
[130] *Id.*
[131] TAYLOR ET AL., *supra* note 7, at 308-14; CASEY, *supra* note 6, at 226-27.
[132] CASEY, *supra* note 6, at 229.
[133] *See Id.*
[134] Luehr, *supra* note 119, at 15.
[135] CASEY, *supra* note 6, at 229.
[136] *See supra* Part III.b.
[137] TAYLOR ET AL., *supra* note 7, at 315; CASEY, *supra* note 6, at 229. The nature and extent of the analysis is also

evidence that are likely to be associated with the crime under investigation, the forensic examiner can more quickly locate relevant evidence.[138] For example, a search for evidence of online auction fraud may first analyze email and image files. In a computer intrusion case the forensic examiner may search for user-created computer source code and computer programs. In narcotics cases, for example, the examiner may be looking for address books and financial records.[139]

However, not all searches are for user-created files, such as documents, email messages or images. Some searches are for system-created data, such as user names, temporary files and printer spool history.[140] Other searches are for file system information, such as directory structure, file attributes, file names, date and time stamps, file sizes and file locations.[141] Such data can answer "who", "what", "when", and "where" questions and can show intent or knowledge. For example, a set of child pornography images neatly organized by a user could be used to show that the possession of those images was not merely the result of something that "just popped up on the screen", but was, in fact, intentional.

In addition to searching for active files, a forensic examiner can search for deleted data. When a file's FAT entry is deleted through the operating system, the underlying data remains on the hard drive until it is overwritten by other data.[142] The deletion of a FAT entry causes the operating system to mark the parts of the hard drive that the file was using as unused (or

---

determined by the legal authority to search, which will be discussed *infra* in part IV.

[138] TAYLOR ET AL., *supra* note 7, at 315.

[139] For lists and tables of crime categories and possible related evidence, *see* U.S. DEPT. OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS 37-44 (2001); *see also* TAYLOR ET AL., *supra* note 7, at 316-18 (listing common evidence by crime type); CYBER FORENSICS: A FIELD MANUAL FOR COLLECTING, EXAMINING, AND PRESERVING EVIDENCE OF COMPUTER CRIMES 54-70 (Albert J. Marcella & Robert S. Greenfield eds., 2002) (discussing various types of evidence from a Windows-based computer).

[140] Luehr, *supra* note 119, at 16-17. In the Microsoft Windows environment the "registry" stores much of the system-created data. *Id.* at 16.

[141] FORENSIC EXAMINATION, *supra* note 50, at 16.

[142] *See supra* Part II.c.

"unallocated").[143] The data in those unallocated parts remains on the hard drive and can be recovered by a forensic examiner using software tools called hex editors.[144] Hex editors allow a forensic examiner to access data at the bit level.[145] Hex editors are named after the manner in which data is displayed within them. Because strings of ones and zeroes are difficult to read, hex editors display data in the hexadecimal numerical format.[146]

Hex editors can also be used to recover partially overwritten files. If the operating system reuses an unallocated part of the hard drive, the data from the new file might only partially overwrite data from a previous file.[147] The portion of the hard drive that is not overwritten by the new data is known as "slack space."[148] It is relatively easy to recover data that is not overwritten at all and remains intact in unallocated space; however, data that has been partially overwritten and that is found in slack space may require the forensic examiner to recreate the file by grafting parts of similar files onto the file fragments.[149] This may give the examiner a sense of the original file, but the grafted file is not the original.[150]

Alternatively, a forensic examiner can compare the file fragments in slack space to a known complete version of the file.[151] Depending on how many parts of the two data sets match, the examiner may conclude that the two files are the same.[152] In such cases, the examiner would need to support such a conclusion with statistics.[153] In particular, the examiner would need to show that there is an infinitesimal probability of the same two combinations of bits occurring by

---

[143] TAYLOR ET AL., *supra* note 7, at 324.
[144] *Id.* at 327.
[145] *Id.* at 328.
[146] *Id.*; s*ee supra* Part III.b. for an explanation of hexadecimal numbers.
[147] TAYLOR, *supra* note 7, at 324.
[148] *Id.* at 324-25.
[149] CASEY, *supra* note 6, at 237.
[150] *Id.*
[151] TAYLOR, *supra* note 7, at 329.
[152] *Id.*
[153] *Id.*

chance.[154]

Even if not deleted, some data may be password-protected, encrypted or compressed, which may indicate an attempt to conceal the data and may be used to show possession or ownership.[155] Nonetheless, such files may be analyzed with the help of other evidence. For example, the password may be found written down near the computer or in unallocated or slack space.[156] In addition, keyboard logging software may be used to collect a computer user's keystrokes – including passwords.[157]

Besides keyboard logging software, other software programs can recover a user password, or decrypt or decompress a file.[158] In fact, there are a variety of forensic software tools available for the analysis of a PC.[159] For instance, disk imaging, write-blocking, hashing and hex editing are accomplished through computer software.[160] Some software programs are all-in-one tools that have all those functions in addition to other searching, analyzing and reporting capabilities. The three most common all-in-one tools currently in use are EnCase, Forensic Toolkit and Ilook.[161]

The use of forensic software tools is encouraged instead of, for example, using an operating system's search function to find files by keyword or file type.[162] A search by keyword is a search based upon a particular word or phrase, and a search by file type looks for certain

---

[154] *Id.*
[155] FORENSIC EXAMINATION, *supra* note 50, at 17; CASEY, *supra* note 6, at 238-39.
[156] CASEY, *supra* note 6, at 239.
[157] *See* John Schwartz, *Compressed Data; Password Protection with Prison Stripes*, N.Y. TIMES, Aug. 6, 2001 (describing sophisticated keyboard logging software developed by the FBI); *see also* United States v. Scarfo, 180 F. Supp. 2d 572 (D. N.J. 2001) (holding that use of keyboard logging software was not an unlawful general warrant in violation of the Fourth Amendment).
[158] E.g., "Password Recovery Tool Kit." FORENSIC EXAMINATION, *supra* note 50, at 27; CASEY, *supra* note 6, at 239.
[159] CASEY, *supra* note 6, at 261-64, 294-301, 326-27; CRIMINAL JUSTICE, *supra* note 1, at 250; TAYLOR, *supra* note 7, at 329-31.
[160] *See supra* Part III.a.
[161] CRIMINAL JUSTICE, *supra* note 1, at 250.
[162] CASEY, *supra* note 6, at 230.

types of files. For instance, in a search for child pornography, the keyword "Lolita" or the file extension "jpg" could be used. However, conducting such searches through the operating system is discouraged, because misleading file names or types may be used, and relevant evidence could be found even in files that are seemingly unrelated to the current investigation.[163] Such problems are avoided through the use of forensic software tools, because they circumvent the operating system and work directly with the data found on the hard drive.[164] Thus, even if a file extension has been changed, a tool such as EnCase can determine the true file type by interrogating the file header, for example.[165]

While searching for data, the forensic examiner is interpreting and analyzing the data "to determine their significance to the case."[166] In some cases, such as child pornography possession cases, the analysis may be relatively straightforward: the examiner may search for and find numerous illegal images on a person's PC. In other cases, however, a more comprehensive analysis may be required, one that involves investigative reconstruction. Investigative reconstruction offers "a more complete picture of a crime" by answering such questions as: what happened, who is responsible, and when, where, how and why the event or events occurred.[167]

Investigative reconstruction in computer forensics falls into six broad categories. First, data hiding analysis is used to determine if a user intentionally concealed data on a PC.[168] This is useful to "indicate knowledge, ownership, or intent."[169] Second, ownership and possession analysis is similar to data hiding analysis in that it seeks to identify the person "who created,

---

[163] *Id.* at 230-31.
[164] HANDBOOK, *supra* note 60, at 53.
[165] *See supra* Part II.c. *See also* CASEY, *supra* note 6, at 230-31; HANDBOOK, *supra* note 60, at 53.
[166] FORENSIC EXAMINATION, *supra* note 50, at 16.
[167] CASEY, *supra* note 6, at 240.
[168] FORENSIC EXAMINATION, *supra* note 50, at 17.
[169] *Id.*

modified, or accessed a file."[170] Third, application and file analysis provides insight into the system's operation "and the knowledge of the user."[171] For example, if files are stored in non-default locations and in an organized manner, this could be used to show knowledge or intent. Fourth, functional analysis assesses how a computer functioned.[172] It answers such questions as: was a computer capable of performing the actions in question and were the actions intentional or the result of a system malfunction?[173] Fifth, relational analysis seeks to "identify relationships between suspects, victim, and crime scene."[174] It can help find other suspects and find connections between various data.[175] Finally, temporal analysis is used to determine "the time and sequence of events."[176] Time-date stamp information is useful because it can be used to associate computer usage to a person or persons at the time the events occurred.[177] It can also be used to create a timeline, which "can help an investigator identify patterns and gaps" in computer activity.[178]

Some of those types of analyses overlap, of course. For instance, while doing a temporal analysis, the forensic examiner must be aware that the user may have intentionally altered the system clock, thus causing time-date stamps to be inaccurate.[179] The examiner should note the difference between the actual and system times and make the appropriate calculations.[180] The examiner could also look to other sources, such as time-date stamps placed on email messages by

---

[170] *Id.* at 18.
[171] *Id.*
[172] CASEY, *supra* note 6, at 241.
[173] *Id.*
[174] *Id.* at 243.
[175] *Id.*
[176] *Id*. at 244; FORENSIC EXAMINATION, *supra* note 50, at 16.
[177] FORENSIC EXAMINATION, *supra* note 50, at 16.
[178] CASEY, *supra* note 6, at 245.
[179] *Id.* at 244.
[180] *Id*.; FORENSIC EXAMINATION, *supra* note 50, at 16-17.

other computers, to determine the actual time of the events.[181] Hence, in doing a temporal analysis, the examiner is also doing a data hiding analysis.

Throughout the forensic examination of a PC, from acquisition to the final stages of analysis, the examiner must document all steps, findings and conclusions.[182] Such "documentation should be contemporaneous with the examination…."[183] This is a prerequisite to creating a final written report and in preparation for possible expert testimony.[184]

IV. THE FOURTH AMENDMENT AND ACCEPTED COMPUTER FORENSIC PRINCIPLES AND METHODOLOGIES

The forensic examination of a computer in criminal investigations must be considered within the legal framework of the Fourth Amendment. The Supreme Court has stated that "the Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance and their memories of the general warrants formerly in use in England."[185] In eighteenth century England, general warrants authorized petty officials to search for seditious papers.[186] Because such papers were not easily identified before the search, general warrants were not specific and gave the officials wide discretion in arresting suspects, searching homes and seizing papers.[187] Similarly, at about the same time in the colonies, writs of assistance authorized local officials – "assistants" of the Crown – to forcibly enter and search a colonist's home for smuggled goods.[188] General warrants and writs of assistance, issued for the convenience of officials, were the "aboriginal subject of the fourth amendment" and were the

---

[181] CASEY, *supra* note 6, at 244-45.
[182] CASEY, *supra* note 6, at 215; FORENSIC EXAMINATION, *supra* note 50, at 19.
[183] FORENSIC EXAMINATION, *supra* note 50, at 19.
[184] *Id.*; CASEY, *supra* note 6, at 249; TAYLOR, *supra* note 7, at 319.
[185] United States v. Chadwick, 433 U.S. 1, 7-8 (1977).
[186] Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 HARV. L. REV. 361, 362-63 (1921).
[187] *Id.*
[188] *Id.* at 364.

evils that the Fourth Amendment was intended to eliminate.[189]

a. Reasonable Expectation of Privacy, Exceptions, and Analogies

Of course, over time Fourth Amendment jurisprudence has evolved to include other considerations besides the ones contemplated when it was drafted. Today, the touchstone in Fourth Amendment analysis is the concept of "reasonable expectation of privacy." If a person has both a subjective and objective reasonable expectation of privacy in a place, then a warrant is required for a state actor to search that place.[190] In other words, a search occurs when there is an infringement upon a person's reasonable expectation of privacy in a place.[191]

In the case of computers, a person may not have a reasonable expectation of privacy in some computer data. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[192] For example, a person may not have a reasonable expectation of privacy in images visible on a computer screen or in data sent over a public network, such as the internet. Even if not sent over the internet, a person may not have an expectation of privacy in data stored locally or even on a private network. For instance, there is probably no reasonable expectation of privacy in email or other data stored on a computer in the workplace that is accessible without a password.[193] Even if access requires a password, there may be no expectation of privacy when the data has been sent across a private network, because in so doing, the data has been knowingly exposed to the system administrator.[194] Furthermore, if

---

[189] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 363 (1974).
[190] California v. Greenwood, 486 U.S. 35, 39 (1988); United States v. Katz, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[191] United States v. Jacobsen, 466 U.S. 109, 113 (1984). Additionally, "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *Id.*
[192] *Katz,* 389 U.S. at 351.
[193] Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 DRAKE L. REV. 239, 243 (2000).
[194] Government agents may search a subscriber's network account pursuant to a system administrator's consent

more than one person has access to data on a computer, then there may be no expectation of privacy in that data.[195]

However, if a person has a reasonable expectation of privacy in computer data, then a warrant is required for law enforcement to search that data – unless the search falls within one of the exceptions to the warrant requirement. There are a number of recognized exceptions to the warrant requirement that may have some application in the computer context, including consent, exigent circumstances, good faith and plain view.

First, if a person consents to the search of his or her computer, then no warrant is required for the part of the search that is within the ambit of the consent.[196] A search could exceed the consent, if, for example, an officer searches a computer's hard drive when a person has only consented to a viewing of what is visible on the computer screen.[197] Second, the exigent circumstances exception could have some application in cases where electronic evidence of a crime is about to be destroyed by a person.[198] In such cases the officer may be justified in seizing the computer without a warrant to prevent the destruction of evidence.[199] However, the officer would nonetheless need a warrant to then search the computer.[200] Third, if an officer reasonably

---

under 18 U.S.C. §§ 2702-2703 (2004) without violating the Fourth Amendment because subscribers have no reasonable expectation of privacy in remotely stored network files. SEARCHING AND SEIZING, *supra* note 2, pt. III. *See also* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *2 (W.D. Wash. May 23, 2001) (holding that Gorshkov did not have a reasonable expectation of privacy in use of a private computer network when he knew that the system administrator could monitor his activities).

[195] This depends on if the person can reasonably expect to retain control over the computer and its data. *See generally* SEARCHING AND SEIZING, *supra* note 2, pt. I.B.3.

[196] *See* United States v. Turner, 169 F.3d 84, 88-89 (1st Cir. 1999) (finding that consent was granted to search for an intruder and evidence of an assault but not for computer files).

[197] *But see* United States v. Lemmons, 282 F.3d 920, 925 (7th Cir. 2002) (holding that when the defendant consented to the search of his trailer, he extended the scope of that consent when he took affirmative steps to help an officer search his computer).

[198] *E.g.*, United States v. David, 756 F. Supp. 1385, 1392 (D. Nev. 1991) (holding that an FBI agent was justified in seizing a handheld computer from which the defendant had deleted a drug price list).

[199] *See* Illinois v. McArthur, 531 U.S. 326, 337 (2001) (holding that the brief warrantless seizure of the defendant's trailer to give the police an opportunity to get a warrant to search within the trailer and to prevent the possible destruction of controlled substances was reasonable).

[200] *See David*, 756 F. Supp. at 1392 (finding that although an FBI agent was justified in seizing a handheld computer

relies on what turns out to be an invalid warrant, the good faith exception applies under federal law.[201] If an officer does not rely on the precise language of the computer search warrant and uses a different search methodology, however, then the officer may not be found to have acted in good faith.[202] Finally, the plain view exception may justify extending the scope of the search of a computer. Some courts have held that if an officer finds evidence of one crime (e.g., child pornography) while searching for evidence of another crime (e.g., controlled substances), the officer must then get a second warrant to continue searching for items not listed in the warrant.[203] Other courts have held that if an officer inadvertently finds evidence of other crimes while searching a computer, then that evidence is considered to be in plain view.[204]

In applying the plain view doctrine to digital evidence, courts have analogized computer searches to searches of closed containers,[205] file cabinets[206] and documents.[207] Of those, the document search analogy is probably the most persuasive. Each collection of bits that makes up a computer file is like a single, physical document, and just as a paper document generally contains a set of related information, so too does the collection of bits that make up a file. Furthermore, analogizing a computer file to a piece of paper is a natural result of how we talk about computer files: we commonly speak of computer files as "documents" or "records."

Because of the way we talk about computers, it is also tempting to analogize a computer to a "container," which is "any object capable of holding another object."[208] In common parlance,

---

to prevent the destruction of evidence, the agent was not authorized to then search the computer); Mincey v. Arizona, 437 U.S. 385, 393-94 (1978) (holding that a warrant was required to search a home once the exigent circumstances had passed).

[201] United States v. Leon, 468 U.S. 897, 918-19 (1984).

[202] United States v. Maxwell, 45 M.J. 406, 420-21 (C.A.A.F. 1996).

[203] *E.g.*, United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999).

[204] *E.g.*, United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

[205] *E.g.*, United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001).

[206] *E.g.*, *Carey*, 172 F.3d at 1274.

[207] *E.g.*, *Gray*, 78 F. Supp. 2d at 529.

[208] New York v. Belton, 453 U.S. 454, 460 n.4 (1981).

a file is said to "in" or "on" a computer. Thus it appears that computers are objects that "hold" other objects, namely computer data. But a computer does not simply hold data, it is *composed* of data. A given computer is the sum total of the data found on that computer's storage device. Without the data, the computer would do little, if anything, when turned on. The closed container analogy is an imperfect one because it conflates two meanings of the word "computer"; it refers to both the physical object and the data as a "computer." For the same reason, the file cabinet analogy also fails: a file cabinet holds various documents, but a computer does not simply hold files – a computer is composed of those files. If we are being precise, we distinguish between a computer *qua* hardware and a computer *qua* electronic data.

There is another reason to reject the container analogy. Closed containers "by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance."[209] The same cannot be said about a computer: one cannot tell its data merely by looking at its hardware. Unlike the contents of a typical closed container, such as a fifty-gallon drum, a kit of burglar's tools or a gun case, the data of a given computer is complex and varied.[210] An officer could infer that the computer "holds" data just by looking at it, but a visual inspection of computer hardware adds nothing to that officer's knowledge of the details of the computer's possible "contents." Hence, the outward appearance of computer hardware in no way diminishes a person's expectation of privacy in the data contained within that hardware – unlike the outward appearance of the usual closed container.

In general, if analogies will be used in computer search cases to help extend existing Fourth Amendment law to new factual situations, then the "intermingled documents" analogy

---

[209] Arkansas v. Sanders, 442 U.S. 753, 764-65 n.13 (1979), *overruled by* California v. Acevedo, 500 U.S. 565 (1991) (overruled on other grounds).
[210] Donald Resseguie, *Computer Searches and Seizure*, 48 CLEV. ST. L. REV. 185, 212 (2000).

will probably be the most helpful.[211] Documents requested in a warrant may be intermingled with documents that are not within the scope of the warrant. As a result, "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[212] Likewise, there may be situations where computer files requested in a warrant may be intermingled with other files. In both cases, because such searches present "grave dangers," "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."[213]

One such way to "take care" is to require a magistrate to intervene where documents requested in a warrant are intermingled with irrelevant documents.[214] "In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, … law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search."[215] In such cases, law enforcement could seize all documents but only search those documents authorized by the supervising magistrate. This approach could be applied to computer search cases, where it appears that the problem of intermingled files that cannot be feasibly sorted on-site is not "comparatively rare."[216]

b. The Warrant Requirement

---

[211] The use of this analogy is predicated on the assumption that on-site searches of computers are too difficult and time-consuming. Analogies are often imperfect and in the case of computers the best analogy may be none at all. *See infra* Part V.
[212] Andresen v. Maryland, 427 U.S. 463, 482 (1976).
[213] *Id.*
[214] United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982).
[215] *Id.*
[216] Resseguie, *supra* note 210, at 207; *see also* United States v. Carey, 172 F.3d 1268, 1275-76 (10th Cir. 1999) (applying a *Tamura* intermingled documents analysis to a computer search case).

In computer search cases, the forensic examination of a computer by a state actor is typically authorized by a valid search warrant.[217] To be valid under the Fourth Amendment, a search warrant must meet three requirements.

First, the warrant must be based on probable cause that evidence of crime will be found in the place to be searched.[218] A showing of probable cause establishes a justification for a search. Probable cause for a warrant exists if there is a reasonable probability that contraband or evidence of a crime will be found in a particular place.[219] The probable cause standard is a "'practical, nontechnical conception.'"[220] "In dealing with probable cause, … as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act."[221]

Establishing probable cause in computer cases requires some showing that evidence will be found in the computer to be searched. This is not always easy in some computer cases. For example, internet service provider records may establish that a certain person sent an email. However, such records may not show which computer the person used to do so. Even if the person has a PC in his or her home, the email may have been sent from another computer at another location.[222] A showing that the person sent the email alone may not establish that he or she sent it from a particular computer.

---

[217] *See, e.g.*, *Carey*, 172 F.3d at 1270 (finding that police had a warrant to search the defendant's computer for evidence related to the sale and distribution of controlled substances); United States v. Triumph Capital Group, 211 F.R.D. 31 (D. Conn. 2002) (finding that the FBI had a warrant to search the defendant's computers for evidence in a public corruption case); United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999) (finding that an FBI agent searched the defendant's four computers with a warrant that authorized a search for evidence of computer intrusions); United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (finding that the FBI obtained a warrant to seize data from American Online ("AOL") accounts suspected of containing child pornography).
[218] U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause….").
[219] Illinois v. Gates, 462 U.S. 213, 231 (1983).
[220] *Id.* (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949)).
[221] *Id.* (quoting *Brinegar*, 338 U.S. at 175).
[222] CYBERCRIME, *supra* note 86, at 78-79.

In addition to being based on probable cause, a valid warrant must be signed by a neutral and detached magistrate who is capable of determining if "probable cause exists for the requested" search.[223] The magistrate must be neutral and detached because law enforcement is engaged "in the often competitive enterprise of ferreting out crime"[224] and "may lack sufficient objectivity to weigh correctly the strength of the evidence supporting the contemplated action against the individual's interests in protecting his own liberty…."[225]

The magistrate need not be an attorney or judge,[226] but must have the "capacity to determine probable cause."[227] Thus, the magistrate must have the experience and training required to determine if probable cause exists.[228] Many aspects of computers are highly technical, so it is unclear what level of expertise is required in computer cases to meaningfully assess a showing of probable cause.. Given that grand and petit juries are often called upon to assess "complex and significant factual data," an experienced judge most likely has the requisite capacity to determine probable cause in computer search cases.[229]

Finally, the warrant must describe with sufficient particularity the place to be searched and the items to be seized.[230] While probable cause establishes justifications for a search, the particularity requirement sets limits on a search. Particularity requires that a warrant be sufficiently precise so that the officer executing the warrant can "with reasonable effort ascertain and identify the place intended."[231] Moreover, "[t]o satisfy the particularity requirement of the

---

[223] U.S. CONST. amend. IV (stating that a warrant must be "supported by Oath or affirmation . . . . "); Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972).
[224] Johnson v. United States, 333 U.S. 10, 14 (1948).
[225] Steagald v. United States, 451 U.S. 204, 212 (1981).
[226] *Shadwick*, 407 U.S. at 349.
[227] *Id.* at 351.
[228] *See id.* (holding that a court clerk has the capacity to determine probable cause in minor municipal offenses).
[229] *Id.*
[230] U.S. CONST. amend. IV ("[W]arrants shall issue . . . . particularly describing the place to be searched, and the persons or things to be seized").
[231] Steele v. United States, 267 U.S. 498, 503 (1925).

fourth amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized."[232] If it is not possible to describe the object of the search in detail beforehand, a search warrant may authorize a search for a class of items. Such generic language is permissible "if it particularizes the types of items to be seized…."[233] However, even if generic, the description must leave nothing to the discretion of the officers.[234]

c. The Particularity Requirement in Computer Searches

The particularity requirement was included in the Fourth Amendment as a remedy to the general warrants and writs of assistance of the colonial period.[235] In light of its history and purposes, the particularity requirement is likely the chief problem in searches and seizures involving computers, for computer searches "can turn into sweeping examinations of a wide array of information."[236] Law enforcement routinely seizes entire computers and computer hard drives, pursuant to computer forensic "best practices." This effectively sets no limit on the search of computers because computers contain a voluminous variety of data – much of which may be personal, private and outside the scope of the investigation.

In executing a "best practices" computer search warrant, the forensic examiner searching a computer may not be able to determine with reasonable effort the place within the computer to be searched. Even if a warrant particularly describes the computer and computer data to be searched, should the warrant particularly describe where on the computer the data is located? It is easy to think of a computer as a single, discrete place to be searched. A laptop is a single item,

---

[232] United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999) (citing United States v. Strand, 761 F.2d 449, 453 (8th Cir. 1985)).
[233] United States v. Layne, 43 F.3d 127, 132 (5th Cir. 1995).
[234] Marron v. United States, 275 U.S. 192, 196 (1927).
[235] ROBERT M. BLOOM & MARK S. BRODIN, CRIMINAL PROCEDURE: EXAMPLES AND EXPLANATIONS 127 (4th ed. 2004); JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROCEDURE 194 (3d ed. 2002).
[236] CYBERCRIME, *supra* note 86, at 154.

and a desktop computer appears to be just a few parts from the exterior. When computer hardware itself is contraband, evidence or an instrumentality or fruit of a crime, then there is little harm in regarding a single computer as a single item. In such cases, the hardware itself may be easily described before the search and identified and seized during.[237] But in cases where computer hardware is merely the storage device for possible evidence and a warrant is sought to search for that data, analogizing a computer to a single place is misleading. Computer storage devices do not contain just one place; they hold multifarious data, such as metadata and user and system files and folders, in numerous small spaces, including bits and bytes and slack and unallocated spaces.

Given the storage capacity of today's computers, a warrant that allows the search of an entire computer could be compared to a warrant that authorizes the search of a home. In some cases, depending on the items sought, the search of an entire home would not be authorized. For example, if there is probable cause to believe that there is a stolen television in the home, the warrant would not authorize the search of desk drawers.[238] Should a computer search warrant have similar limitations to comport with the rationale and history of the particularity requirement?[239]

If relying on a container analogy, then a "best practices" search of every place within a computer without further description is probably justified, because an officer with authority to search a place for an item has the authority to search any containers or spaces in the place that

---

[237] SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.a.
[238] United States v. Ross, 456 U.S. 798, 820-21 (1982).
[239] "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be that the Constitution affords no protection against such invasions of individual security?" Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

are large enough to contain the item.[240] "A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found, and is not limited by the possibility that separate acts of entry or opening may be required to complete the search."[241] Each place in a computer could be compared to a small space or container that an officer is justified in "opening" because it might contain an item sought.[242]

However, there are good reasons to reject the closed container analogy and follow an intermingled documents analogy instead.[243] Under an intermingled documents analysis, the search of an entire computer would, in some cases, require the intervention of a neutral and detached magistrate. The magistrate would review the discrete places within a computer to determine if a forensic examiner might search those places. This approach has the advantage of protecting privacy interests, but the costs are high: the magistrate must have at his or her disposal technical expertise to review data, and such a review may introduce inefficiencies into computer search cases.

There is another particularity problem with a "best practices" computer search warrant. By allowing the seizure of an entire computer and the search of all data contained therein, such a warrant leaves a great deal to the discretion of a forensic examiner. A single computer can store a vast amount of information – much of which may be totally irrelevant to the investigation. From

---

[240] *Id.* Furthermore, under the container analogy an officer is probably justified in searching a computer, even if the computer is not specifically authorized by a warrant, if an item that the officer is authorized to seize could be within the computer data. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("[T]he scope of a lawful search is defined by the object of the search. . . .") (internal quotation marks omitted); *see also* United States v. Gomez-Soto, 723 F.2d 649, 655 (9th Cir. 1984) ("The failure of the warrant to anticipate the precise container in which the material sought might be found is not fatal.").

[241] *Ross*, 456 U.S. at 820-21.

[242] *See* David J. S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 863 (2005) ("[A]n officer conducting a search for evidence on a defendant's computer should have the authority under a warrant to open and view any document on the computer's hard drive to the extent necessary to determine if the document is within the warrant's purview, because any document could contain material described in the warrant.").

[243] *See supra* Part IV.a.

this arises the question: what data should be searched and what property should be seized? In other words, how much discretion should a forensic examiner have in a computer search case? Without any further limitations on the search, a warrant that allows the search of "any computers and computer media located therein," for instance, will leave most of the decision on how to search to the discretion of the examiner.

Courts have sought to limit a forensic examiner's discretion in the search of a computer by requiring the inclusion of a "search strategy" in the warrant.[244] A search strategy is a recitation of how law enforcement officials will conduct the search of a computer. The inclusion of such language is an additional, non-Constitutional element of the particularity requirement. The particular manner in which a computer will be searched is included in the warrant or affidavit, in addition to the particular description of the place to be searched and the items to be seized. Hence, a search strategy not only authorizes the search for particular items, it also limits how a forensic examiner may go about searching for those items. For example, a search strategy warrant could authorize a forensic examiner to search for possible evidence through the use of specific keyword searches.[245] In such cases, the warrant or affidavit would describe the particular keywords to be used to search for files containing a certain word or file extension.

Search strategies are not a panacea for the particularity problems of computer searches,

---

[244] For example, Massachusetts Superior Court Judge Paul A. Chernoff held that in computer search cases, "the affidavit must set out the specific parameters of the requested search as present technology eliminates in many cases the need for law enforcement's exposure to and examination of each and every file during a computer search, unlike the physical document search of a file cabinet. Of course, in some cases, all of the electronic files in a particular program should be examined. For example, a search for specific check records could reasonably involve a review of all the entities in a financial management program such as 'Quicken,' although in some cases time parameters as to record entries might be appropriate. For those cases where entire files need not be reviewed, executing officers should utilize keyword searches, provided that the established probable cause exists for each keyword... Some files may not be susceptible to keyword search. In such a case, the affidavit must bring this to the attention of the magistrate who may elect to authorize a file search that is broader in scope than a key word search." Amy Baron-Evans & Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 B.B.J. 10, 12 (2003).

[245] *See supra* Part III.c for a description of keyword searches.

however. An affidavit may contain a search strategy that follows computer forensic "best practices" by authorizing an off-site search of all data on a computer's hard drive. In such cases, the search strategy does very little, if anything, to limit law enforcement's search of the data and to satisfy the Fourth Amendment's particularity requirement. In fact, the Department of Justice recommends that all computer search warrant affidavits include a search strategy because "explaining the search strategy in the affidavit helps to counter defense counsel motions to suppress based on the agents' alleged 'flagrant disregard' of the warrant during the execution of the search."[246] Moreover, agents should avoid "articulating an excessively narrow or restrictive search strategy" because "defense counsel may also allege flagrant disregard of a warrant if agents transgress the strategy described in the warrant."[247]

Despite the particularity problems of "best practices" computer searches, a number of federal courts have upheld such searches. For example, in *United States v. Campos*,[248] the Tenth Circuit upheld the seizure of a defendant's computer hardware and the subsequent off-site search of all its data for child pornography.[249] The defendant argued that the search of his entire computer constituted a general search, but the court concluded that the search did not violate the Fourth Amendment because the warrant was sufficiently particular in that it authorized a search for "items relating to child pornography."[250]

Similarly, in *United States v. Lacy*,[251] the defendant argued that a warrant authorizing the seizure of all his computer equipment was "too general."[252] The Ninth Circuit found that the

---

[246] SEARCHING AND SEIZING, *supra* note 2, pt. II.C.
[247] *Id.*
[248] United States v. Campos, 221 F.3d 1143 (10th Cir. 2000).
[249] *Id.* at 1147.
[250] *Id.* at 1146-47. Although inapplicable to the facts of the instant case, the court recommended an intermingled documents approach in some cases. *Id.* at 1148. *See supra* Part IV.a for an explanation of the intermingled documents approach.
[251] United States v. Lacy, 119 F.3d 742 (9th Cir. 1997).
[252] *Id.* at 746.

warrant "contained objective limits to help officers determine which items they could seize"[253] because the warrant authorized agents to seize only the data that was linked to a Danish computer system.[254] Although the warrant "described the computer equipment itself in generic terms and subjected it to blanket seizure," the court found such a description and seizure justified because "a Customs agent [had] explained [that] there was no way to specify what hardware and software had to be seized…."[255]

In *United States v. Scott-Emuakpor*,[256] the court found that the police did not flagrantly disregard a warrant by seizing computer hardware and data that were not specifically described in the warrant.[257] The court also found that the seizure of those items did not amount to a prohibited general search.[258] The seizure of items not listed in the warrant was justified because "agents had no way of knowing whether [the evidence] would be found on computer hard drives or on zip disks; nor did they know the format in which those files might be stored."[259] Furthermore, the seizure of those items for an off-site search was "reasonable because it allowed the agents to preserve the computer system as it existed for the computer analysts, who were not present during the search…."[260]

d. New Rules for Computer Searches?

---

[253] *Id.*
[254] *Id.* at 745-46.
[255] *Id.* at 746-47.
[256] United States v. Scott-Emuakpor, No. 1:99-CR-138, 2000 U.S. Dist. LEXIS 3118 (W.D. Mich. Jan. 25, 2000).
[257] *Id.* at *17-18; *see also* United States v. Sissler, No. 1:90-CR-12, 1991 U.S. Dist. LEXIS 16465, at *7, *11-12 (W.D. Mich. Aug. 30, 1991) (following a container analogy to conclude that the police seizure and off-site search of over five hundred computer disks and a PC did not flagrantly disregard the warrant, which had authorized the seizure of records involving drug transactions).
[258] *Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, at *19.
[259] *Id.*; *see also* United States v. Lamb, 945 F. Supp. 441, 458-59 (N.D.N.Y 1996) (upholding a warrant that authorized the seizure and off-site search of all of a defendant's America Online email files, including files that did not contain child pornography, because "the actual content of a computer file usually cannot be determined until it is opened with the appropriate application software on a computer").
[260] *Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, at *19.

The judicial sanctioning of "best practices" computer searches has encroached on the penumbra of protections afforded by the Fourth Amendment. This has led Professor Orin Kerr to conclude that existing Fourth Amendment rules that first found life and application in the physical world sometime "permit extraordinarily invasive government powers to go unregulated in some contexts."[261] Hence, Professor Kerr argues that the new methods of gathering digital evidence trigger a need for new legal standards and "rules of criminal procedure that restore the function of the old rules given the new facts."[262]

Kerr compiles a list of traditional rules that are problematic when applied to computer searches. First, "the traditional rule [that investigators cannot seize property beyond the scope of probable cause] requires a level of surgical precision and expertise that is possible for physical evidence but not digital evidence."[263] Second, Kerr avers that under traditional rules, making a copy of computer files is not a "seizure" and analyzing that copy is not a "search."[264] "Because police can create a perfect copy of the evidence without depriving the suspect of property, the new facts unhinge the rule from its traditional function of limiting police investigations."[265] Third, the particularity requirement fails to limit government intrusion in computer searches. "Given how much information can be stored in a small computer hard drive, the particularity requirement no longer serves the function in electronic evidence cases that it serves in physical

---

[261] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005). Those same rules also a sometimes "allow phantom privacy threats to shut down legitimate investigations in other[]" contexts. *Id.*

[262] *Id*. at 314. In response to Kerr others have argued that no new rules are needed and that existing rules are sufficient to balance public safety concerns against privacy rights. *See, e.g.*, Ziff, *supra* note 242, at 841 (arguing "that courts should address the novel problem of computer searches by not treating it as a novel problem at all, but by simply applying established case law that controls the search of personal documents"). For instance, Ziff argues that the plain view exception in computer cases is limited by the "immediately apparent" doctrine: computer data can be seized only if its incriminating character is immediately apparent to an examining officer. That doctrine serves to limit the search of the computer data and thus protect privacy rights. *Id*. at 866.

[263] Kerr, *supra* note 261, at 300.

[264] *Id.* at 301.

[265] *Id.*

evidence cases."[266] Next, the rule that allows investigators executing a warrant to look in any place where evidence described in the warrant could conceivably be located "imposes a substantial limit for physical searches, but not for searches for electronic evidence," because electronic evidence could be located anywhere on a hard drive.[267] Finally, Kerr argues that the plain view exception under existing law effectively makes all computer searches general searches.[268] Under *Horton v. California*,[269] if evidence is found in plain view during an objectively justifiable search, then that evidence is admissible.[270] The search of an entire hard drive is almost always objectively justifiable because electronic evidence could be located anywhere on the hard drive.[271]

Kerr notes that courts have sometimes recognized those problems with existing Fourth Amendment rules and have crafted new rules because computer searches have been found to be "special,"[272] "unique,"[273] or "different."[274] On the one hand, many of the new rules serve to sanction "best practices" computer searches. For instance, one newly "ossified"[275] rule is that "[a] valid warrant entitles investigators to seize computers and search them off-site at a later date."[276] On the other hand, some of the new rules seek to offer Fourth Amendment protections where traditional rules have failed to do so. For example, requiring the inclusion of a "search strategy"

---

[266] *Id.* at 303.
[267] *Id.* at 304.
[268] *Id.* at 305.
[269] Horton v. California, 496 U.S. 128 (1990).
[270] *Id.* at 138. The plain view exception does not require inadvertent discovery; an officer could intend to find one class of evidence even if the warrant authorizes a search only for another class of evidence. *Id.* Thus, the subjective intent of the officer is not determinative in a plain view analysis. *Id.*
[271] Kerr, *supra* note 261, at 305. For the sake of completeness, it should be noted that Kerr also argues that traditional Fourth Amendment law "imposes no time limits on computer searches and pays little attention to when or whether seized computers must be returned" because such law focuses on property not privacy interests. *Id.* at 305-06.
[272] United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).
[273] United States v. Barbuto, No. 2:00CR197K, 2001 U.S. Dist. LEXIS 25968, at *10 (D. Utah Apr. 12, 2001).
[274] People v. Gall, 30 P.3d 145, 156 (Colo. 2001) (Martinez, J., dissenting).
[275] Kerr, *supra* note 261, at 315.
[276] *Id.*

in a warrant is a new rule that seeks to restore the particularity requirement in computer searches.[277] In addition, courts have – contrary to the holding of *Horton* – looked to the subjective intent of an officer to give meaning to the plain view exception in the computer context.[278]

Kerr argues that the creation of new rules for computer searches should continue in order to address the Fourth Amendment problems of computer searches – the Federal Rules of Criminal Procedure should be amended, Congress should pass new laws and courts should implement new rules.[279] Furthermore, Kerr asserts that the changes must be "institutional" and not merely incremental.[280] For example, Kerr suggests that the plain view exception to computer searches could be abolished to prevent *de facto* general warrants in computer searches.[281] Small changes, such as requiring greater specificity in computer search warrants, will fail to restore the "lost functionality" of Fourth Amendment rules.[282]

Kerr declares that traditional Fourth Amendment rules, which germinated in the physical world, require law enforcement to undertake steps that are not possible[283] or "impractical"[284] in the computer world. Kerr's solution is to create new institutional rules. In suggesting such a solution, Kerr does not consider whether the way computers are searched should change; instead, he assumes that the constitutional and other legal rules that govern such searches should change.

---

[277] *Id.* at 316. *See supra* Part IV.c.
[278] Kerr, *supra* note 261, at 316-17. Kerr discusses *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (suppressing child pornography evidence because the officer's subjective intent showed that he had changed the scope of the search from narcotics evidence to child pornography) and *United States v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999) (admitting child pornography evidence because an investigator's continued search of a hard drive was permissible, even after he found images of child pornography, because the investigator intended to search for evidence of computer hacking only) and compares those two cases to *Horton v. California*, 496 U.S. 128, 138 (1990), where the United States Supreme Court held that the subjective intent of an officer is irrelevant in applying the plain view exception.
[279] Kerr, *supra* note 261, at 306-17.
[280] *Id.* at 308.
[281] *Id.* at 314.
[282] *Id.* at 303.
[283] *Id.* at 300.
[284] *Id.* at 315.

Thus, his arguments are based on the assumption that the only way to seize and search electronic evidence is by following current computer forensic "best practices." Kerr is tacitly agreeing with law enforcement that the only methods available are those methods that are currently in widespread use.

Kerr demonstrates that the rules of criminal procedure are "organic" and have changed, and will continue to change, based upon new factual situations.[285] Accordingly, institutional changes may be required. However, until such changes are implemented, law enforcement, defendants, attorneys and trial courts have little guidance in determining how to balance governmental and privacy interests in the area of computer searches. In addition to any long-term modifications to, and growth in, Fourth Amendment jurisprudence, there is a relatively simple solution to computer search problems that can be implemented immediately – instead of changing the law to follow forensic examination practices, such practices could change to accord with the law. This will require judges and defense attorneys to challenge law enforcement to work harder to use computer forensic examination methods that respect Fourth Amendment rights. Such methods in the end may require few new legal standards or rules of criminal procedure.

V. ALTERNATIVES TO CURRENT COMPUTER FORENSIC "BEST PRACTICES"

a. Do We Need Acquisition, Authentication, and Analysis as We Know It?

Accepted computer examination principles and methodologies drive how warrant applications are drafted and reviewed and "considerations of practicality" justify law

[285] Kerr, *supra* note 261, at 281. "Whichever device, precedent or legislation, is chosen for the communication of standards of behaviour, these, however smoothly they work over the great mass of ordinary cases, will, at some point where their application is in question, prove indeterminate; they will have what has been termed an *open texture*." H.L.A. HART, THE CONCEPT OF LAW 124 (1961) (emphasis in original).

enforcement actions in computer searches.[286] There are, however, available alternatives to current computer forensic "best practices." This part offers some concrete proposals for modifications to current computer forensic methodologies. Specifically, this part discusses alternatives that address overly broad computer searches and particularity problems in computer search warrants.[287]

There is a technological reality that is overlooked when drafting "best practices" warrants – on-site searches of computer data are not difficult and time-consuming anymore. Perhaps at one time, in the early days of computing, such searches were fraught with difficulties, such as slow hardware and unstable software. And although computers continue to be imperfect in many ways, and in comparison with the operation of other consumer electronics, PCs have evolved and improved since the days of black screens, green characters and clock speeds measured in the single-digits.[288] Today, searching for relevant data on a computer hard drive is highly efficient compared to, for instance, searching for a physical document in a file cabinet.[289] In some cases a physical document may be found quickly, but physical searches for documents are ultimately slower, more difficult and complicated than similar searches for electronic data.[290] Consider the

---

[286] *See* United States v. Sissler, No. 1:90-CR-12, 1991 U.S. Dist. LEXIS 16465, at *12 (W.D. Mich. Aug. 30, 1991) ("Like the seizure of documents, the seizure of the computer hardware and software was motivated by considerations of practicality. Therefore, the alleged carte blanche seizure of them was not a 'flagrant disregard' for the limitations of a search warrant.") (internal citations omitted).

[287] *See supra* Part IV.c.

[288] For example, 4.77 MHz was the clock speed of the CPU in the first PC, which was introduced on August 12, 1981 by International Business Machines ("IBM"). MUELLER, *supra* note 21, at 23. Clock speed is the measurement of the rate of the CPU's clock signal and is expressed in megahertz ("MHz") and gigahertz ("GHz"). *Id.* at 412, 1371. The clock signal synchronizes every operation of a CPU. *Id.* Thus, a faster clock speed results in a more frequent clock signal, which results in more CPU operations in a shorter amount of time. *Ceteris paribus*, a faster clock speed equals a faster computer. Clock speed can also be measured in seconds: the clock speed of the original IBM PC was 1.33 nanoseconds, yet the clock speed of a relatively slow computer in 2005 equipped with a 1.5 GHz CPU is about one half of that at 0.67 nanoseconds. *Id.* at 412-13. Overall, a 1.5 GHz Pentium IV-based PC is nearly 12,000 faster in processing speed (not just clock speed) than the original IBM PC. *Id.* at 23.

[289] *See* Resseguie, *supra* note 210, at 209-10 ("[S]earching for relevant documents on a computer hard drive, with the aid of search engines and utility programs, may actually be more efficient than manually searching through a large paper file cabinet unaided by technology.").

[290] Thus, case law that supports off-site searches of paper documents on grounds of practicality is mostly

ease with which the entire internet is searched from a single PC located in a home – type in a few carefully chosen words about a given subject in a search engine, hit the enter key and a set of links to relevant web pages is promptly displayed. If a particular web page is viewed, then the contents of that page can be searched quickly and easily using a web browser's find function.[291]

In the case of computer forensics, searches for electronic data are now aided by forensic software packages such as EnCase.[292] Such software can be used to search efficiently and effectively for possible evidence on-site.[293] In particular, forensic software can identify and separate known data through file hashing and can classify unknown data by file type.[294] Concerns about missed evidence because of changed file extensions or misleading file names are unfounded when using such software, because the software interrogates the data directly and looks to metadata, such as file headers, to determine file types and contents.[295] Thus, there is no need for a warrant to authorize law enforcement to look at all data on a storage device when searching for evidentiary data – law enforcement need only search classes of data that are

---

inapplicable to the computer context. *See* United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (holding that there was no flagrant disregard because the "wholesale seizure of file cabinets and miscellaneous papers . . . . was motivated by the impracticability of on-site sorting and the time constraints of executing a daytime search warrant"); Crooker v. Mulligan, 788 F.2d 809, 812 (1st Cir. 1986) (noting cases "upholding the seizure of documents, both incriminating and innocuous, which are not specified in a warrant but are intermingled, in a single unit, with relevant documents"); United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982) (finding that a suppression motion was properly denied "where the Government's wholesale seizures were motivated by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing'"); United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982) (stating that "[i]f commingling prevents on-site inspection, and no other practical alternative exists, the entire property may be seizable, at least temporarily").

[291] Similarly, searches of online databases can be faster and easier than searches of hardcopy library materials. For instance, an online search for a word's definition, synonyms, antonyms, and usage examples is swift and simple compared to a corresponding search through printed versions of Webster's dictionary, the Oxford English Dictionary, and Roget's Thesaurus.

[292] *See supra* Part III.c.

[293] An analysis PC loaded with the appropriate software could be attached to, and could be used to search, an evidence PC or storage device on-site.

[294] *See supra* Part III.b. In a way, the software could be said to be "searching" all the data on a storage device in order to classify that data; however, this methodical computational winnowing protects privacy interests better than the alternative of having a human law enforcement officer rummage through the entire contents of a storage device.

[295] *See supra* Parts II.c., III.c. It is probably true that if law enforcement has more time to search (i.e., if hardware is seized and the data is searched at a leisurely pace in a lab), then there is less of a chance of missed evidence. But if law enforcement is limited by time during on-site searches and some evidence is missed, then that evidence is just like any other form of evidence that is overlooked. Such a possibility must be balanced against privacy rights.

relevant to the investigation.[296] For instance, in a child pornography case, a warrant could authorize a forensic examiner to search through data with image file headers, but not through data with text document headers.

In light of the technological realities of computing today, in particular the celerity and accuracy with which computer data can be searched using forensic software tools, law enforcement claims that on-site searches for digital evidence are overly time-consuming and impractical are disingenuous at best.[297] Thus, in applicable circumstances, warrants should authorize on-site computer searches only. Clearly, such searches can be conducted with a minimal risk of missed evidence and in a timely manner using readily available software tools.

Because on-site searches are feasible, computer search warrants should, instead of authorizing the seizure of hardware for an off-site search, authorize the seizure of only the relevant electronic data found on the hardware, unless the hardware itself is contraband, evidence or an instrumentality or fruit of a crime.[298] In practice, the only way to seize a subset of data on a storage device is to copy that data. Accordingly, such warrants should authorize the copying of only the data that is relevant to the investigation.[299] Despite law enforcement claims to the

---

[296] The specific classes of data to be searched should be supported by probable cause. *See supra* note 244. For example, the search for deleted data may require a showing of probable cause to believe that there is relevant evidence within the class of deleted data. Deleted data can be readily identified and found by forensic software. *But see* United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) (refusing to analogize deleted images to trash on the street, *see* California v. Greenwood, 486 U.S. 35, 40 (1988), but holding that a search for deleted images was within the scope of the warrant even though not specifically authorized by the warrant, because recovering the deleted files was "no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note"). Nonetheless, it could be argued that the deletion or hiding of data may support the assertion of a heightened expectation of privacy in that data. *See* United States v. Villarreal, 963 F.2d 770, 773 (5th Cir. 1992) (suggesting that persons "can manifest legitimate expectations of privacy" by concealing items).

[297] *See* SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.b ("[I]t may take days or weeks to find the specific information described in the warrant because computer storage devices can contain extraordinary amounts of information.").

[298] *See supra* Part IV.c; s*ee also Upham*, 168 F.3d at 535 (holding that if evidence "could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of *all* computer equipment, a category potentially including equipment that contained no [evidence] and had no connection to the crime") (emphasis in original).

[299] Law enforcement typically seeks to copy an entire hard drive. One reason given for such a request is that the

contrary, there is no need to seize the original data (which results in the seizure of storage devices and all the data contained therein), because copies of electronic data can be authenticated using individual file hashing.[300] Individual file hashing can thus be used to show the accuracy of electronic copies for evidentiary purposes.[301] Moreover, accurate duplicates and printouts of electronic data are admissible under the Federal Rules of Evidence.[302]

In sum, a new "best practices" search warrant should authorize the on-site search for a particular class or classes of data, and seizures of only the data that is relevant to the crime being investigated. In doing so, the warrant would respect Fourth Amendment rights while authorizing effective law enforcement activities that are technologically possible and practicable.

VI. CONCLUSIONS

In the physical world, Fourth Amendment standards are easily applied. A neutral and detached magistrate finds probable cause and issues a search warrant describing in detail the place to be searched. For instance, a search warrant may authorize a police officer to search for controlled substances in a person's home at a certain time. The officer may not seize the entire contents of the home, carry them away and then search through them at his leisure. His search is

---

mirror image will allow a forensic examiner to inspect the data without altering the original. *See supra* Part III.a for some other reasons in support of for disk imaging; *see also* CASEY, *supra* note 6, at 226 ("[A]lways make at least two copies of digital evidence"); CYBERCRIME, *supra* note 86, at 106 ("[A]lways make a mirror image"); TAYLOR, *supra* note 7, at 309 ("With any seized system, it is important to create a working copy for forensic analysis"). However, in other contexts law enforcement routinely "alters" physical items in order to search or seize them. For example, part of a carpet found in a home may be cut away so that bloodstains can be examined in a lab. The entire carpet is not rolled up and carried away; instead, only the portion of carpet that contains evidence is seized. At the lab, the analysis of the bloodstains may alter them. Such changes to the evidence are accepted as a part of the forensic examination process and are, *a fortiori*, a primary consideration when deciding the order in which various analyses should be done.

[300] *See supra* Part III.b.

[301] When making copies or analyzing data, law enforcement should use write-blockers to prevent unnecessary alteration. *See supra* Part III.a. Software tools such as EnCase have built-in write-blocking capabilities. *See supra* Part III.c.

[302] FED. R. EVID. 1001, 1003. "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'." *Id*. at 1001. *See, e.g.*, CONN. CODE EVID. § 10-2 ("A copy of a writing, recording or photograph is admissible to the same extent as an original ….").

limited by the contents of the warrant.

In the computer context, however, the particularity requirement has seemingly been abandoned. Search warrants for computers could be likened to the general warrants and writs of assistance that the particularity requirement of the Fourth Amendment was intended to eliminate. Under current "best practices," computers (which can store massive amounts of data) are seized, taken off site and then rummaged through by forensic examiners. On-site searches for particular computer files are too "complicated" [303] and may take "days or weeks."[304] The needs of law enforcement – and not Fourth Amendment rights – control the content of warrants.

This state of affairs has been accepted, or at least tolerated, because computer searches are seen as "special." In many ways, the computer world is unlike the physical one. As a result, courts have struggled to apply to the computer world Fourth Amendment law that was developed from cases in the physical world. One solution is to create new Fourth Amendment rules for computer searches. Alternatively, law enforcement could use methods that comport with the Fourth Amendment and current technology allows law enforcement to do so. The details of the accepted trilogy of acquisition, authentication and analysis could be reworked in favor of preserving Fourth Amendment rights. Thus, the forensic examination of computers would follow from the law, and not vice versa.

[303] SEARCHING AND SEIZING, *supra* note 2, pt. II.A.
[304] SEARCHING AND SEIZING, *supra* note 2, pt. II.B.1.b.