

***531 SEARCHES AND SEIZURES IN A DIGITAL WORLD**

Orin S. Kerr [\[FNa1\]](#)

* * *

***536 I. The New Facts of Computer Searches and Seizures**

* * *

The process of retrieving evidence from a computer is known as computer forensics. [\[FN19\]](#) It is mostly experts' work; computer forensics analysis typically is performed pursuant to a search warrant by a trained analyst at a government forensics laboratory. [\[FN20\]](#) Weeks or ***538** months after the computer has been seized from the target's home, an analyst will comb through the world of information inside the computer to try to find the evidence justifying the search. She will use a range of software programs to aid the search, which can take many days or even weeks to complete. These tools help analysts sift through the mountain of data in a hard drive and locate specific types or pieces of data. Often they will uncover a great deal of detailed evidence helping to prove the crime; in a few cases, the search will come up empty. In a number of cases, the search for one type of evidence will result in the analyst stumbling across evidence of an unrelated crime. [\[FN21\]](#)

Computer searches and home searches are similar in many ways. In both cases, the police attempt to find and retrieve useful information hidden inside a closed container. At the same time, significant differences exist. * * * This Part explores four basic factual differences between home searches and computer searches: the environment, the copying process, the storage mechanism, and the retrieval mechanism.

A. The Environment: Homes vs. Hard Drives

The traditional focal point of Fourth Amendment law is physical entry into a home. [\[FN22\]](#) Homes offer predictable, specific, and discrete physical regions for physical searches. Investigators can enter through a door or window and can walk from room to room. They can search individual rooms by observing their contents, opening drawers and other containers, and looking through them. The basic mechanism is walking into a physical space, observing, and moving items to expose additional property to visual observation. Enter, observe, and move.

Computer storage devices are different.

* * *

While houses are divided into rooms, computers are more like virtual warehouses. When a user seeks a particular file, the operating system must be able to find the file and retrieve it quickly. To do this, operating systems divide all of the space on the hard drive into discrete subparts known as "clusters" or "allocation units." [\[FN29\]](#) * * * Just as a filing cabinet might store particular items in a particular place in the warehouse, the operating system might use a cluster to store a particular computer file in a particular place on the hard drive. The operating system keeps a list of where the different files are located on the ***540** hard drive; this list is known as the File Allocation Table or Master File Table (MFT), de-

pending on the operating system. [FN31] When a user tells his computer to access a particular file, the computer consults that master list and then sends the magnetic heads over to the physical location of the correct cluster. [FN32]

The differences between homes and computers prompt an important question: what does it mean to “search” a computer storage device? In the physical world, entering a home constitutes a search. [FN33] Merely observing a room does not constitute a search, but opening containers and cabinets to look inside does. [FN34] * * * Retrieving information from a computer means entering commands that copy data from the magnetic discs, process it, and send it to the user. When exactly does a search occur?

B. The Copying Process: Private Property vs. Bitstream Copies

A second difference between home and computer searches concerns ownership and control over the item searched. When a police officer searches a home, the home and property he searches typically belong to the target of the investigation. Indeed, some sort of legitimate relationship between the property searched and the defendant is needed to generate Fourth Amendment rights. [FN35] Once again, computers are different. To ensure the evidentiary integrity of the original evidence, the computer forensics process always begins with the creation of a perfect “bitstream” copy or “image” of the original storage device saved as a “read only” file. [FN36] All analysis is performed on the bitstream copy instead of the original. [FN37] The actual search occurs on the government's computer, not the defendant's.

* * *

The accuracy of the bitstream copy often is confirmed using something called a “one way hash function,” or, more simply, a “hash.” [FN40] A hash is a complicated mathematical operation, performed by a computer on a string of data, that can be used to determine whether two files are identical. [FN41] If two nonidentical files are inputted into the hash program, the computer will output different results. [FN42] If the two identical files are inputted, however, the hash function will generate identical output. * * *

C. The Storage Mechanism: Home vs. Computer Storage

A third important difference between computers and homes concerns how much they can store and how much control people have over what they contain. Homes can store anything--including computers, of course--but their size tends to limit the amount of evidence they can contain. A room can only store so many packages, and a home can only contain so many rooms. Further, individuals tend to have considerable control over what is inside their homes. They can *542 destroy evidence and usually know if it has been destroyed. Computers can only store data, but the amount of data is staggering. * * *

The storage practices of computers prompt an important legal question: how can Fourth Amendment rules limit and regulate the scope of computer searches? The Fourth Amendment was created to abolish general warrants and require narrow searches. Can the rules that limit physical searches also apply to computer searches, or are new rules needed?

D. The Retrieval Mechanism: Physical vs. Logical

The fourth difference between home searches and computer searches concerns the techniques for finding evidence and the invasiveness of routine

searches. Executing a physical search of a home generally requires assembling and training a search team. Police officers look from room to room for the evidence sought in the warrant. If the evidence sought is large, the police will limit their search accordingly: if they are looking for a stolen car, for example, they can't look inside a suitcase to find it. [FN51] The police may conduct unusually thorough searches in particularly important cases, but such searches are costly and relatively rare. After the police have searched the space for the item sought, the search is done, and the police will leave. * * *

In contrast to physical searches, digital evidence searches generally occur at both a “logical” or “virtual” level and a “physical” level. The distinction between physical searches and logical searches is fundamental in computer forensics: while a logical search is based on the file systems found on the hard drive as presented by the operating system, [FN55] a physical search identifies and recovers data across the entire physical drive without regard to the file system. [FN56] Because of the need to conduct both physical and logical searches, the computer search process tends to be more labor intensive and thorough than the physical search of a home. Consider a search for a picture file believed to be evidence of a crime. An examiner might begin by conducting a logical search of the hard drive for files with extensions known to be used for image files, such as “.jpg.” [FN57] The forensic analyst could direct his software to consult the Master File Table for any files with the extension “.jpg,” and then either list these files or automatically present “thumbnail” images of those files for viewing. Forensic software generally facilitates the latter with a simple command. For example, the current version of the EnCase forensic software has a feature called *545 “Gallery View.” [FN58] If an analyst selects a hard drive or folder to be searched and then clicks the “Gallery” button, the software looks for all files ending with a picture file extension and automatically presents thumbnails of those files to the user. [FN59]

This procedure sounds easy, but ordinarily does not suffice. It is easy to change the extension of a file. To hide a picture, a user might take a file saved with a “.jpg” extension and resave it with an extension common to a different kind of file, such as “.doc” or “.wpd.” [FN60] A search for picture files based on the logical file extensions will no longer locate the file. Instead, the analyst will have to conduct a search at a physical instead of logical level. Software can locate image files at a physical level by searching for file headers characteristic of known types of picture files. A file header is a segment of data that informs the operating system about the associated file; in the case of a picture file, the file header would contain data indicating that the file is a photograph of a particular type and dimension. [FN61] The file header remains unchanged regardless of the extension placed on the file, allowing a physical search to uncover picture files that a logical search would not locate. In addition, file header characteristics can be located in slack space or in partially deleted files, allowing a skilled analyst to reconstruct the file and recover the associated picture. [FN62] The process can be tremendously time consuming, however. Searching an entire hard drive for elements of file headers can take weeks, and it is easy for an analyst to overlook elements. [FN63] * * *

Analysts can also locate specific images, files, and applications by using the one way hash function mentioned earlier. The National Drug Intelligence Center has calculated and collected common hash values for nearly every known application and operating system file and for many images of child pornography in a database called the Hashkeeper. [FN66] Many forensic analysts also compile their own databases of hashes known to be associated with specific types of files. If there is a match between the hash of a known file in a database and a file located in the computer being searched, an analyst can be confident that he has identified

a particular file without actually opening or looking at it. Once the analyst has located a file, he can record information about the file retained by the operating system, such as MAC times, [\[FN67\]](#) and the folder in which it was found. * * *

The differences between computer searches and traditional physical searches raise difficult questions about the rules that should govern computer searches and seizures. Generally it is more difficult to plan a computer search *ex ante*; the search procedures are more contingent than procedures for physical searches, and they are more of an art than a science. The search can require a very time-consuming and invasive process in every case, and the costs of a comprehensive search are substantially lower. The question is, should these dynamics impact the rules that courts use to review the scope of computer searches--and if so, how?

* * *

III. The Fourth Amendment and Data Reduction

[W]e can now turn to the subsequent data reduction stage. During this phase, investigators search through an image of the suspect's computer for specific evidence related to a crime. In most of these cases, the police will have obtained a search warrant authorizing the search. But many questions about the scope of the warrant remain. What steps can the police take to find the evidence named in the warrant? What kinds of searches pursuant to a warrant are "reasonable," and what kinds are "unreasonable"? Which rules should regulate *ex ante* what steps the police can take, and which rules should regulate *ex post* the admissibility of the files they discover?

A. Reasonableness and Physical Evidence Collection

Investigators looking for one type of evidence often come across something else incriminating. Perhaps an officer looking through a suspect's pocket for a driver's license instead finds drugs. Or perhaps *567 an officer looking inside a car for drugs instead comes across a gun. In some cases, the discovery of the latter evidence is inadvertent. In others, the officer's conduct is a pretextual search designed to discover the evidence subsequently obtained. Creating a legal rule to govern admissibility of the latter evidence is difficult because no clear line separates cases where use of the extra evidence simply helps the police fight crime from cases where use of the extra evidence encourages abusive law enforcement practices. * * *

*568 The plain view doctrine is the legal rule that balances the competing concerns of protecting public safety and preventing misuse of government power in this context. In its current form, the plain view doctrine permits the police to seize evidence discovered during a valid search if the incriminating nature of the item to be seized is immediately apparent. [\[FN160\]](#) The fairly broad scope of the doctrine reflects a judgment that the dynamics of physical evidence collection render the risk of pretextual and dragnet searches relatively low. *Horton v. California* [\[FN161\]](#) provides a useful illustration. In *Horton*, the Supreme Court held that the plain view exception justifies a search even if the officer had the subjective intent to execute a pretextual search. [\[FN162\]](#) This rule was permissible because other aspects of physical evidence collection already served to thwart general searches. First, "[s]crupulous adherence" to the requirement that the police particularly describe the place to be searched and thing to be seized made it unlikely that police would use the plain view exception as a means to conduct

general searches. [FN163] Second, the fact that police could only look in places and containers large enough to contain the specific physical evidence sought necessarily limited the scope of warrantless searches. [FN164]

B. Reasonableness and Digital Evidence Collection

The realities of the computer forensics process present a very different dynamic, suggesting a significantly higher risk of general searches. This is true for several reasons. First, the virtual nature of digital evidence weakens or eliminates the two traditional limits on searches and seizures identified in Horton. In the case of searches with warrants, digital evidence diminishes the regulatory effect of the particularity requirement. [FN165] The particularity requirement reflects a physical concern: the thinking is that the law can limit searches by confining where in the physical world the police search and by naming the object of the search. Searching for data on a hard drive upsets *569 these assumptions. A warrant to seize a computer hard drive is sufficiently particular under existing standards--the computer itself is small--but an entire virtual world of information may be stored inside it. * * *

Second, computers are playing an ever greater role in daily life and are recording a growing proportion of it. In the 1980s, computers were used primarily as glorified typewriters. Today they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more. As computers become involved in more aspects of our lives, they record increasingly diverse information. Each new software application means another aspect of our lives monitored and recorded by our computers. * * *

Third, computer searches tend to be unusually invasive. A search for one type of digital evidence often reveals a tremendous amount of other evidence: a great deal comes into plain view. * * * [C]omputer searches are much less expensive and less time-pressured than traditional physical searches. While comprehensive home searches are possible, their cost and inconvenience makes them the exception rather than the rule. * * * In contrast, a single computer analyst can conduct a very invasive search through a computer at any time. * * * Computer searches lower *570 the cost and inconvenience of invasive searches, making such searches the norm rather than the exception.

* * *

D. Rethinking the Plain View Doctrine

* * *This section argues that the best way to neutralize dragnet searches is to rethink the plain view exception in the context of digital evidence. The dynamics of computer searches upset the *577 basic assumptions underlying the plain view doctrine. More and more evidence comes into plain view, and the particularity requirement no longer functions effectively as a check on dragnet searches. In this new environment, a tightening of the plain view doctrine may be necessary to ensure that computer warrants that are narrow in theory do not become broad in practice. * * *

1. Approaches That Focus on the Circumstances of the Search.--One approach to narrowing the traditional plain view exception would factor in the circumstances of the search. For example, one method would involve overturning Horton and restoring the inadvertence requirement, placing the emphasis on the analyst's subjective intent. Another method would entail regulating the par-

ticular tools used during the forensic search; for instance, this approach might require the police to use particularly advanced forensic tools. Yet another method would permit plain view evidence when the specific forensic step that *578 uncovered it was “reasonable,” but not if the step was unreasonable. All of these proposals have surface appeal, but on deeper reflection prove unpromising.

Two courts already have refashioned the plain view exception in the context of computer searches so that it focuses on the analyst’s subjective intent. In *Carey* and *United States v. Gray*, [FN201] forensic analysts looking for one kind of information came across digital images of child pornography. In *Carey*, the analyst stopped looking for drug evidence and began to look for child pornography; [FN202] in *Gray*, the analyst continued to look for evidence of computer hacking but in doing so discovered more child pornography. [FN203] In both cases, the courts focused on the subjective intent of the officer to either stay within or look beyond the scope of the warrant. When the officer looked for evidence described in the warrant, the discovered images could be used in court; [FN204] when the officer looked beyond the warrant, the images were suppressed. [FN205]

The subjective approach followed by the *Carey* and *Gray* courts offers one significant advantage over the existing objective test: it turns the emphasis from a question judges are poorly equipped to answer (the reasonableness of a particular forensic step) to a question judges are better positioned to answer (witness credibility). Judges are familiar with physical searches; they can understand how searches occur and what steps agents might take. Armed with this knowledge, judges can use objective tests to distinguish steps that are consistent with a search for evidence from steps that are characteristic of general searches. Judges have little sense of how to distinguish a reasonable forensics process from an unreasonable one, however. The technical details are too complex and fluid. In this environment, a subjective test may serve as a second-best proxy for the objective test. Although judges may be poorly equipped to assess whether in fact an analyst’s steps were consistent with a targeted search, they are better able to tell whether the analyst was at least attempting to conduct a good faith targeted search.

However, the subjective approach has a critical weakness. An officer’s subjective intent may be difficult to discern. Proving intent is particularly problematic in the computer context because government agencies can set policies that mandate very thorough forensic investigations. For example, the FBI has generally trained its forensic analysts*579 to conduct highly comprehensive examinations; the default practice is to leave no digital stone unturned. [FN206] Such a policy can create General Tool through practice instead of technology. When every step taken by an analyst is a matter of routine policy, it becomes difficult to exclude evidence on the ground that the analyst was attempting to circumvent the warrant. Reliance on agency policy may explain *Gray*, in which the agent testified that he kept searching for evidence named in the warrant after repeatedly coming across other evidence because he was simply following FBI forensic policies. [FN207] The existence of otherwise laudable standardized practices makes the subjective intent approach much less helpful in practice than it first seems in theory.

Another option is for the law to require the use of certain tools instead of others. If the police can conduct a search using either Perfect Tool or General Tool, for example, perhaps the law should require use of Perfect Tool. The problem with this approach is that it does not provide a judicially manageable standard. * * *

Another possibility would hinge admissibility of plain view evidence on whether the particular forensic step that led to the evidence was reasonable or unreasonable given the government’s needs, the extent of the privacy violation, and the relevant legal authority. [FN209] Under this approach, plain view evi-

dence discovered during reasonable searches would be admitted, while such evidence discovered during unreasonable searches would be suppressed. Such a case-by-case approach*580 is an interesting option, but it may be difficult for courts to apply. * * *

2. Approaches That Focus on Future Uses of the Evidence Obtained.--Another approach that has considerable surface appeal would hinge admissibility of evidence on the type of evidence obtained and its usefulness in other prosecutions. Perhaps the plain view doctrine should permit the use of evidence only for serious crimes, or only for terrorist offenses, but not allow evidence to be used for low-level offenses. * * *

*581 This is a possible approach, but also a problematic one. First, it is quite difficult to draw an *ex ante* line between compelling cases and low-level cases. We tend to know the difference when we see it, but it is surprisingly hard to draw the distinction using a legal rule. Say we are most worried about terrorism cases, and the rule is that the government can only use plain view evidence to prosecute terrorism. This prompts a difficult question: what is a “terrorism” case? There is no federal crime of “terrorism.” Instead, the U.S. Code contains a number of criminal offenses that may be used in terrorism-related cases. [\[FN215\]](#) Is any case that involves any one of these crimes a terrorism case? Can any evidence of any of these crimes justify the introduction of plain view evidence, even if it is not particularly probative? Given that some of these statutes are worded quite broadly, can the government use plain view evidence simply by raising one of the terrorism crimes as one of several charges in a multi-count indictment, even if the alleged conduct does not seem to be primarily terrorism-related?

Second, any rule that hinges governmental power on the type of offense creates a strong incentive for Congress to expand the list of eligible offenses over time, watering down the protection. If plain view evidence is admissible only in terrorism cases, for example, Congress will have an incentive to broaden the category of terrorism crimes. * * *

Finally, settling on a list of specific crimes that should qualify to admit plain view evidence proves quite difficult. It is hard enough to come up with a single rule that best balances law enforcement concerns against fears of pretextual or abusive investigations for all crimes. Coming up with different rules for different sets of crimes is *582 exponentially more complicated. * * *

3. Abolishing the Plain View Exception?--This brings us to the simplest but also most draconian approach: the plain view exception could be abolished for digital evidence searches. Courts could apply a *583 very simple rule, suppressing all evidence beyond the scope of a warrant--or, in the case of warrantless searches, evidence unrelated to the justification for the search--unless the traditional independent source or inevitable discovery doctrine removed the taint. [\[FN223\]](#) This approach would permit forensic investigators to conduct whatever searches they deemed necessary, and to use General Tool or its equivalent however they liked, with the caveat that only evidence within the scope of the warrant normally could be used in court. Dragnet searches would be neutralized by a rule ensuring that only evidence within the scope of proper authority could be used. Statutory privacy rules resembling the nondisclosure rule for grand jury testimony would presumably be needed to supplement this protection; [\[FN224\]](#) such rules could ensure that evidence beyond the scope of a warrant was not only never used in court, but also never disclosed. [\[FN225\]](#)

It is too early for courts or Congress to impose such a rule. Many of the characteristic dynamics of computer searches identified in this Article are trends gradually becoming more significant with time. A decade ago, courts could simply and accurately analogize computers to other closed containers; today, the analogy seems a stretch, and a decade from now, it will probably seem obviously flawed. The need for new rules is emerging, but eliminating the plain view ex-

ception would be too severe at present. As time passes, however, that will likely change. Abolishing the plain view exception may become an increasingly sound doctrinal response to the new dynamics of digital evidence collection and retrieval.

In time, abolishing the plain view exception may best balance the competing needs of privacy and law enforcement in light of developments in computer technology and the digital forensics process. [\[FN226\]](#) Forensic analysis is an art, not a science; the process is contingent, technical, and difficult to reduce to rules. Eliminating the plain view exception in digital evidence cases would respect law enforcement interests by granting the police every power needed to identify and locate evidence within the scope of a warrant given the particular context-sensitive needs of the investigation. At the same time, the approach would protect privacy interests by barring the disclosure of any evidence beyond the scope of a valid warrant in most cases. It is ***584** an imperfect answer, to be sure, but it may be the best available rule. * * *