Warrant Searches of Computers

Jeff Welty
School of Government
May 2011

I. Searches of Computers Are Increasingly Important

Computers now permeate all strata of society and all aspects of people's lives. Unsurprisingly, then, computers are often used to commit, or contain evidence of, crimes. This is obviously true of computer-specific crimes, such as the computer fraud and computer trespass crimes in G.S. 14-453 et seq. It is also true of a category of crimes that, while theoretically not computer-specific, are in fact committed almost exclusively by means of or with the assistance of a computer. The production, distribution, and possession of child pornography is a prime example, but identity theft and certain forms of intellectual property piracy also fall in this category. Furthermore, computers may play a part in the commission of, or may contain evidence of, crimes that are not inherently tied to computers at all, such as murder (one recent case involved evidence that the defendant had Googled "how to dispose of a body"), drug distribution (computers may contain customer lists), and the like.

This paper focuses on searches of computers pursuant to a search warrant. Probable cause to support the issuance of a search warrant may arise in any number of ways. A spouse, roommate, or computer repairperson may accidentally discover child pornography on a suspect's computer and report it to police. See, e.g., State v. Dexter, 186 N.C. App. 587 (2007). A police officer posing as a minor may communicate with a sexual predator over the internet. See, e.g., State v. Ellis, 188 N.C. App. 820 (2008). Or, police may have developed probable cause to search a home for evidence of a crime, and may seek to search a computer simply as one facet of the broader search. See, e.g., State v. Peterson, 179 N.C. App. 437 (2006), aff'd, 361 N.C. 587 (2007). Of course, similar fact patterns may arise with respect to cellular phones or other electronic devices, and the legal principles discussed below will also apply to such devices.

While this paper is written with a North Carolina audience in mind, our appellate courts have decided relatively few cases concerning searches of computers. Therefore, most of the cited cases are federal cases, to which our trial and appellate judges might reasonably look for guidance.

II. Apparent and Concealed Data

Although this paper is not intended to be technical, it is worth describing briefly the ways in which data can be stored on a computer. Sometimes, computers contain valuable evidence that is stored in an obvious location, such as pirated music stored in the user's music library. But computers may also contain valuable evidence in less-obvious locations. And sometimes, computers contain evidence that users have gone to great lengths to hide or delete. Thus, rather than simply clicking through the file directory on a computer, law enforcement may seek authorization to search the computer using sophisticated forensic software – or may employ such software without specific authorization.

A. Apparent Files

Virtually all computers contain word processing documents, spreadsheets, and other files created by office or productivity software. Many contain photographs, videos, and audio files. Many have financial records created using Quicken or other financial software. A typical user makes no effort to hide these files, and any computer user who inspected the computer would be able to locate them easily. Using the Windows operating system, for example, the typical user will save word processing files in the "My Documents" folder, or a subfolder therein. If the documents are created in Microsoft Word, they will be associated with a Word logo and will carry a .doc or .docx file extension. The typical user will name files descriptively; in other words, she will use a name like "June 2010 letter to the editor" for a letter written to a local newspaper.

If a computer has ever been used for web browsing, it will also normally contain information about at least some of the web sites it has visited. Obtaining this information requires a little more computer knowledge than, say, viewing a word processing document as described above, but not much, at least in some instances. For example, most web browsers have a history feature. The browser saves a list of all the web sites the computer has visited over the past few weeks or months, and upon command, the browser can display the list. Similarly, many web sites use "cookies" – small files automatically saved on the user's computer when the user first visits a particular web site – as a way of recognizing repeat visitors. Looking at the cookies saved on a computer will reveal many web sites recently visited by the computer. Other forms of temporary internet files may also be found on most computers.

B. Camouflaged Files

If a user has information on his or her computer that the user does not want others to see – such as a spouse, a computer repair technician, or law enforcement – he may take steps to camouflage the files. At the simplest level, giving a file a misleading title, such as saving a child pornography photograph as "familyvacation002.jpg" may provide some concealment. Another common technique is changing the file extension. Saving a child pornography photograph as "familybudget.xls" will make it look like a Microsoft Excel Spreadsheet to the casual observer.

C. Encrypted Files

More sophisticated users may use encryption to prevent others from accessing their files. An encrypted file is one that has been saved using a special code so that the file is unreadable unless it is decoded – and it cannot be decoded without a password. The codes used by the best modern encryption systems are practically unbreakable. Thus, if the police seize and search the computer of a drug dealer who stores all his business records and customer lists in encrypted word processing documents, they are not likely to obtain any readable, useful evidence unless they can guess the drug dealer's password.[1]

[1] For an interesting case concerning encryption and the ability of the prosecution to compel the defendant to provide data in an unencrypted form or to provide an encryption password, see United States v. Boucher, 2009 WL 424718 (D. Vt. Feb 19, 2009).

D. Deleted Files

Many computer users believe that once a file has been deleted, it is gone and cannot be recovered. In fact, when a file is deleted, the disk space where that file was stored is marked "available" by the operating system, but the file is not actually erased. Unless and until the disk space is actually used to save another file, the previous file remains on the disk, even though the operating system has "officially" marked the file as deleted. (It is a bit like removing the card catalog card for a book, but leaving the book on the shelf.) Given that most people have large amounts of empty space on their disk drives, and save additional items to disk infrequently, deleted files often remain on disk drives for weeks, months, or years. A computer analyst can look through a disk drive using special software and find these deleted files.

Even if the area of the disk that was previously used to store the deleted file has been used to store a new file, some portion of the deleted file may remain. Disk drives are divided into chunks, or sectors, and most files take up a fraction of a sector (whether 2.04 sectors, or 40.77 sectors, the point is that most files don't take up exactly 3.00 or 158.00 sectors). When a file that took up 2.87 sectors is "deleted," and the disk space is later overwritten by a new file that takes up 2.12 sectors, only 12% of the third sector used by the new file is actually overwritten. Since the deleted file used 87% of that third sector, there is still a fragment of the deleted file on the disk, and a computer forensic analyst will be able to locate that fragment and see what it contains.

If a sector has been completely rewritten with a new file, or has been "zeroed," i.e., written over by a computer with meaningless material, the deleted file probably cannot be recovered using current technology. However, it may be possible in the future to recover part or all of the deleted file even under these circumstances.[2]

E. Other Evidence

There are other ways to recover information from a computer. For example, some recently-used information may be stored in the computer's RAM, for ready access. And because the field of computer forensics is rapidly evolving, additional ways of extracting information from computers (as well as additional ways of hiding or removing such information) are sure to be invented. Indeed, with the rise of solid-state disk drives (SSDs), which record and delete information in a slightly different way than traditional spinning hard disks, new techniques are certain to emerge.

III. Many Computer Searches Require a Warrant

Generally, people have a reasonable expectation of privacy in the contents of their computers. See, e.g., United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325 (6th Cir.

[2] While computers are extremely precise, they are not quite perfect, and so when the computer is writing over the disk space used by the deleted file, it may not completely obliterate the previous material. For example, the disk head may be in an infinitesimally different position than when the deleted file was written on the disk, leaving a "shadow" along the edge of the track where the previous magnetic charge remains, as if a typist used a slightly-too-thin correction ribbon that did not quite obliterate the erroneous text.

2001).[3] Thus, searches of computers normally must be conducted pursuant to a warrant, unless an exception to the warrant requirement applies. For example, the police may legally search computers without a search warrant when the owner of a computer consents to a search, or when the police have probable cause to believe that a computer contains evidence of a crime and exigent circumstances require that the police search the computer immediately. Such warrantless searches are beyond the scope of this paper, but are discussed elsewhere.[4]

In some instances, it may be prudent, or even necessary, to issue multiple warrants to search a single computer. For example, suppose that the police develop probable cause to believe that a person is involved in accounting fraud, and obtain a warrant to search his computer for evidence of that offense. Then, while reviewing documents saved on the computer, an officer inadvertently discovers evidence of child pornography. If the officer wants to continue looking for child pornography, at least in files and locations that are not likely to contain evidence of accounting fraud (such as video files, perhaps), he may need a separate search warrant authorizing a search for child pornography. This issue is discussed below in Section VI.B of this paper.

IV. Showings of Probable Cause

An application for a warrant to search a computer must establish probable cause to believe that the computer contains evidence of, or was used in, a crime. Although probable cause is a familiar standard, there are several specific, recurrent issues that arise with respect to computer search warrants.

A. Does the probable cause extend to computers?

First, just because there is probable cause to search a location for evidence of a crime, it does not automatically follow that there is probable cause to search any computers found at that location. See, e.g., State v. Peterson, 179 N.C. App. 437 (2006), aff'd, 361 N.C. 587 (2007) (although there was probable cause to search a residence for evidence of a homicide, there was no probable cause to search computers at the residence; "[t]he affidavit does not include any indication . . . that would suggest a search of defendant's computer would lead to information regarding the potential homicide"). A judicial official evaluating an application for a search warrant that expressly authorizes the search of one or more computers should, of course, consider this issue. A judicial official evaluating an application for a search warrant that does not specifically address whether computer searches are permitted – for example, a search warrant that authorizes the search of a residence for evidence of drug trafficking – may also wish to consider this issue. If the judicial official determines that there is probable cause to issue the warrant

[3] There are exceptions to this rule. For example, when an individual chooses to install file-sharing software on her computer, and thereby makes its contents widely accessible, she may relinquish her expectation of privacy in the computer's contents. Serious questions also may arise about a user's expectation of privacy in a workplace computer, and about a user's expectation of privacy in a stolen or misappropriated computer. A number of cases on the expectation of privacy issue are collected in Jeff Welty, Warrantless Searches of Computers and Other Electronic Devices, April 2011 (available online at http://sogweb.sog.unc.edu/blogs/ncclaw/?p=2179).

[4] Jeff Welty, Warrantless Searches of Computers and Other Electronic Devices, April 2011 (available online at http://sogweb.sog.unc.edu/blogs/ncclaw/?p=2179).

but that the probable cause does not extend to any computers in the location to be searched, he or she may modify the language of the warrant accordingly.

B. Staleness

When an officer applies for a search warrant based on information that is several weeks or months old, the judicial official should consider whether the information continues to provide probable cause or whether it has become outdated, or "stale." This issue has been litigated most often in connection with child pornography cases. Some courts have recognized that people who obtain child pornography tend to hoard, or retain it, meaning that evidence that a person obtained digital child pornography months, or even years, ago may provide probable cause to believe that the person's computer will contain child pornography. See, e.g., United States v. Allen, 625 F.3d 830 (5th Cir. 2010) (evidence of possession of child pornography that was 18 months old was not stale where officer's affidavit asserted (a) that people who possess child pornography tend to maintain their collections over time and (b) that deleted files can often be recovered much later); United States v. Potts, 586 F.3d 823, (10th Cir. 2009) (evidence that defendant possessed child pornography 10 months prior to the issuance of the warrant was not stale because (a) the defendant vaguely acknowledged a continued interest in child pornography just before the warrant issued and (b) the court found that collectors of child pornography tend to hoard it); United States v. Frechette, 583 F.3d 374 (6th Cir. 2009) (evidence that defendant subscribed to a child pornography website 15 months prior to the issuance of a search warrant was not stale and provided probable cause); United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) ("Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them."). Other courts have been less willing to find probable cause based on information that is not recent, at least absent a specific reason to believe that the particular suspect at issue is likely to have retained the pornographic images. See, e.g., United States v. Greathouse, 297 F. Supp. 2d 1264 (D. Or. 2003) (evidence that, thirteen months prior to the issuance of a search warrant, the defendant shared child pornography from his computer with other people over the internet was stale; there was no evidence of more recent, or ongoing, criminal activity; no evidence that the defendant was a pedophile and so especially likely to hoard such material; and computer technology evolves quickly, so that whole hard drives become obsolete or are replaced frequently; the court also noted that the government presented no empirical evidence that people who obtain child pornography are prone to keep it for protracted periods); cf. United States v. Zimmerman, 277 F.3d 426 (3d Cir. 2002) (police suspected that the defendant had showed a single adult pornography video to minors six, ten, or more months earlier; they applied for and obtained a search warrant authorizing a search of the defendant's computers for child and adult pornography; the Third Circuit ruled that there was nothing at all to support a search for child pornography, and as to adult pornography, the evidence was stale; there was no reason to believe that the defendant would have kept the video for a long period of time, since unlike child pornography, it was presumably legal and easy to obtain; the court also expressed doubt about the utility of boilerplate affidavits about the tendency of pedophiles to hoard child pornography absent some knowledge of the specific defendant and case).

C. Descriptions of child pornography

Many computer search warrants are issued based on probable cause to believe that the suspect's computer contains images of child pornography. Sometimes the officer seeking the warrant has seen the

images himself, while sometimes he has not viewed the images but has been told about them by, for example, someone who lives with the suspect. In order for a judicial official to make an independent determination about whether the images are likely child pornography, the judicial official probably must (1) view the images (they may be attached to application in a sealed envelope), or (2) receive a detailed description of the images that allows the judicial official to reach an independent conclusion about the content of the images. A statement from the applicant that the images "are child pornography" is probably insufficient, as it does not provide factual information that the judicial official can use to determine probable cause. See, e.g., United States v. Brunette, 256 F.3d 14 (1st Cir. 2001) (an officer determined that the defendant had posted several images online; the officer applied for a search warrant for the defendant's computer, describing the images only as "a prepubescent boy lasciviously displaying his genitals," parroting the language of 18 U.S.C. §2256(2)(E), which defines such genital displays as child pornography; the reviewing court held that description was conclusory and failed to provide probable cause; generally, "[a] judge cannot . . . make this determination without either a look at the allegedly pornographic images, or at least an assessment based on a detailed, factual description of them"); United States v. Battershell, 457 F.3d 1048 (9th Cir. 2006) (defendant's girlfriend showed a police officer several pictures she had found on defendant's computer; the officer then applied for a warrant to search the computer for child pornography; he did not attach the images; he described the images as showing "a young female (8-10 YOA) naked in a bathtub" and "another young female having sexual intercourse with an adult male"; the reviewing court found that the former description was insufficient to show probable cause that the computer contained child pornography, as opposed to, say, a family photograph, but that the latter was sufficient, especially combined with the girlfriend's statement that the computer had pictures of "kids having sex"; although it "would have been preferable if the affiant in this case had included copies of the photographs in the warrant application," an officer's failure "to include a photograph in a warrant application is not fatal to establishing probable cause"). But cf. United States v. Miknevich, __ F.3d __, 2011 WL 692973 (3rd Cir. Mar. 1, 2011) (although the "better practice for an applicant seeking a warrant based on images of alleged child pornography to append the images or to provide a description of the images," probable cause was established here based on the descriptive and explicit file name listed in the application as well as the file's SHA1 value); United States v. Krupa, 633 F.3d 1148 (9th Cir. 2011) (initial consent search revealed a picture of a nude teenage girl; although alone insufficient to provide probable cause to support search warrant for child pornography, combined with other factors such as the presence of 15 computers and two children in a "disheveled" home, it was enough); United States v. Harner, 2009 WL 2849139 (D. Minn. Sept. 1, 2009) (unpublished) (finding probable cause based on officer's estimate that video depicted 13 to 15 year old; alternatively, based on hash value of images on defendant's computer); Ferrick v. State, 217 P.3d 418 (Alaska Ct. App. 2009) (description of pictures of naked children, albeit not totally ruling out the possibility that the images were artistic or were not of real children, was adequate to provide probable cause); United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998) (warrant application established probable cause to believe that the defendant's computer would contain child pornography despite failure to attach or describe images, where the defendant had engaged in online "chat" with undercover officer and had offered to supply computer disks with images of pre-pubescent children engaged in sexual activity).

V. The Scope of the Warrant

Another area in which computer search warrants can be tricky concerns the scope of the search authorized by the warrant.

A. Is computer-specific language needed?

First, although a warrant must particularly describe the location to be searched, it does not always need to include computer-specific language to authorize the police to search computers. The general rule is that a warrant authorizing the search of a particular location for a particular item also authorizes the search of any closed container at the location if the item might reasonably be found inside the container. Wayne R. LaFave, Search and Seizure § 4.10(b) (4th ed. 2004); cf. United States v. Ross, 456 U.S. 798 (1982) (expressing a similar rule as to warrantless vehicle searches). Thus, a warrant authorizing the search of a home for records of drug sales, lists of drug customers, etc., also authorizes the search of any container within the home in which the records could reasonably be found. Several courts have applied this rule to hold that a warrant need not specifically refer to the existence of a computer in order to authorize a search of the computer, so long as the items or evidence sought might reasonably be found on the computer. See e.g., United States v. Giberson, 527 F.3d 882 (9th Cir. 2008) (holding that a search warrant authorizing a search for "documents," without mentioning computers or electronic storage, allowed police to search computers, as documents may be found in computers); United States v. Hudspeth, 459 F.3d 922 (8th Cir. 2006), rev'd in part on other grounds, 518 F.3d 954 (8th Cir. 2008) (en banc) (upholding a computer search conducted pursuant to a warrant allowing the search of any and all "records or documents regarding sales, payables, inventory, customer lists, financial statements, and personnel files" but not specifically mentioning computers: "While the inclusion of the word 'computer' would have specified one location among several where the officers might look for those items, its omission did not prevent the officers from searching [a] computer for such records."); cf. United States v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998) (proper for warrant to authorize search of computers although nothing in the warrant application showed that the records the police sought were specifically likely to be stored on computer; most business records and documents are stored that way). But see United States v. Payton, 573 F.3d 859 (9th Cir. 2009) (suggesting that computer-specific language normally is required).

B. Which computers may be searched?

When confronted with a warrant application that does contain computer-specific language, a judicial official should carefully consider whether the probable cause that supports the warrant extends to the particular computers or other devices in question. This issue is discussed to some extent above, in Section IV.A of this paper. Compare, e.g., United States v. Hill, 459 F.3d 966 (9th Cir. 2006) (after computer repair technician reported finding child pornography on defendant's computer, police obtained warrant for, inter alia, "all storage media belonging to either the computer or the individual identifying himself as defendant" at defendant's home; defendant argued that the warrant was overbroad, i.e., that it authorized the seizure of items for which there was no probable cause; the court agreed, holding that blanket seizures of all computer-related items in a particular place will often be justified because there is no way to know where a specific file or image is located, but that the affiant must say as much, and since the affiant did not do so here, the warrant was overbroad), with, e.g., United States v. Summage, 481 F.3d 1075 (8th Cir. 2007) (police suspected that the defendant had paid a mentally handicapped man to engage

in a sex act with a woman, and had videotaped and photographed the encounter; officers obtained warrant for "[a]ll video tapes and DVDs . . . [a]ll video and/or digital recording devices and equipment . . . [and] computer(s)"; found child pornography during the search; court held that there was probable cause to believe that the video and photographs would be stored digitally, and that the officer had no way to know the format or device in which the video and photographs would be found, and that it was therefore reasonable to believe that the video and photographs might be present in any of the digital media); United States v. Grimmett, 439 F.3d 1063 (10th Cir. 2006) (upholding warrant that authorized the search of "any computer equipment" and "any and all computer software" for child pornography; LEO testified that he actually searched only in types of files likely to contain child pornography, such as .jpg and .gif files; thus the search was not an improper "general" search; query whether the officer's conduct in executing the warrant can cure the overbreadth of the warrant).

C. Description of the property to be seized

Search warrants must particularly describe the property to be seized, i.e., what the officers are hoping to find. When dealing with computer search warrants, it is important to recognize that files or data, not the physical computers themselves, are usually the objects of the search.[5] (Of course, the physical computers themselves may be need to be seized, taken offsite, and examined, as discussed later in this paper.) Thus, a computer search warrant should describe the files or data as specifically as possible – "files containing customer lists and drug transaction records" or "still images or video footage of child pornography." However, courts have recognized that computer searches are similar to searches for incriminating documents, in that officers often do not know exactly what type of information the search will uncover. Thus, courts have allowed somewhat flexible descriptions. See, e.g., United States v. Burke, 633 F.3d 984 (10th Cir. 2011) (search warrant authorizing officers to seize "computers" "hard drives" and "media storage" was sufficiently particular because the warrant stated that the defendant was suspected of the sexual exploitation of children; that brought "to officers' attention the purpose of the search" and effectively limited its object); United States v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998) (upholding a warrant authorizing a search of a suspect's office and computer for documents related to money laundering; the warrant was sufficiently specific because it identified a particular offense and included an illustrative list of types of documents that would be relevant; although officers would have to make some judgments about which documents met the description, and would necessarily scan many irrelevant documents, no greater specificity was possible in advance). This flexibility is not infinite; search warrants that have not limited the items to be seized to, for example, evidence of a particular offense have been held to lack particularity. See, e.g., United States v. Rosa, 626 F.3d 56 (2nd Cir. 2010) (police obtained computer search warrant based on suspicion that the defendant was sexually abusing and photographing children; warrant authorized search for "computer equipment, electronic digital storage media," and the like; the warrant itself did not "set forth the nature of the suspected criminal activity" or otherwise limit the scope of the search; it therefore lacked particularity, though the court held that the good faith exception applied); Mink v. Knox, 613 F.3d 995 (10th Cir. 2010) (warrant that authorized "the search and seizure of all computer and non-computer equipment and written materials in Mr. Mink's

[5] There are exceptions to this rule. For example, if a suspect is believed to have stolen a particular computer during a break-in, and the police obtain a search warrant for suspect's home, the computer itself would be an object of the search, regardless of what files or data it might contain.

house, without any mention of any particular crime to which they might be related" lacked particularity); United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) (warrant in child pornography investigation authorized officers to search defendant's computer "and all electronic and magnetic media stored therein"; the warrant did not specifically state that the search was limited to evidence of child pornography offenses, and "thus permitted the officers to search for anything – from child pornography to tax returns to private correspondence"; it was therefore lacking in particularity and was invalid, though the court ultimately found the search to be permitted under the good-faith exception); United States v. Cioffi, 668 F.Supp.2d 385 (E.D.N.Y. 2009) (search warrant allowing search of a suspect's Gmail account insufficiently particular as it did not limit the emails to be seized to those relevant to the specific charged securities crimes; although the application detailed what was sought, the application was not incorporated into the warrant).

D. Authorization for off-site examinations

As noted above, officers will often want to seize a suspect's computers and take them off-site to search them, perhaps in a law enforcement computer laboratory and with the assistance of specialized personnel and software. Courts have often found this to be justifiable, partly as a matter of simple practicality: a complete forensic analysis of a computer can take weeks, and it would be burdensome (to the police) and intrusive (to the computer's owner) to insist that the police remain on-site for the entire time. See, e.g., United States v. Hill, 459 F.3d 966 (9th Cir. 2006) (officers obtained a search warrant to search the defendant's computer and storage media for child pornography; they seized all his disks, etc., for off-site analysis; he argued that they should have been required to search the storage media on-site and release anything that didn't contain child pornography; both the district court and the reviewing court held otherwise, concluding that it was reasonable, given the difficult, time-consuming nature of computer searches, to take the computers off-site; the district court ruled that the defendant was entitled to copies of his data, which would ameliorate the hardship of the seizure). It is probably wise for officers to seek authorization in the search warrant to seize the computers and analyze them off-site. See United States v. Grimmett, 439 F.3d 1063 (10th Cir. 2006) (upholding warrant where the "affidavit also made clear that the search of the computer would be off-site in a laboratory setting" because only careful laboratory analysis allows all relevant evidence to be exploited); United States v. Mutschelknaus, 592 F.3d 826 (8th Cir. 2010) (warrant allowing officers 60 days to conduct off-site examination of seized computer was reasonable given the complexity of computer searches).

E. Inclusion of a search protocol

Finally, there has been considerable debate about whether a warrant authorizing the search of a computer should include a "search protocol" that explains how the police intend to go about searching the computer. The idea is that most computers contain vast amounts of innocent, but personal, information intermixed with any incriminating information, and that the police should demonstrate that they plan to search the computer in a way that is calculated to minimize the invasion of privacy vis-à-vis the former while unearthing the latter. Although an important early case suggested that such a protocol might be required, see United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), more recent cases generally hold otherwise, see, e.g., United States v. Khanani, 502 F.3d 1281 (11th Cir. 2007) (search protocol not required); United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005) ("[W]e disagree with [the defendant]

that the government was required to describe its specific search methodology. This court has never required warrants to contain a particularized computer search strategy.").

VI. Execution of the Warrant

A. May the entire computer be searched?

Generally, courts have held that when a warrant authorizes the search of a computer, it authorizes at least a cursory review of every file on the computer. This is because of the ease with which files can be camouflaged or disguised, as discussed above in Section II of this paper. See, e.g., United States v. Stabile, 633 F.3d 219 (3rd Cir. 2011) (searching video files pursuant to search warrant for financial crimes was "objectively reasonable because criminals can easily alter file names and file extensions to conceal contraband," and "the plain view doctrine applies to seizures of evidence during searches of computer files, [though] the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner"); United States v. Williams, 592 F.3d 511 (4th Cir. 2010) (stating that a computer search requires "at least a cursory review of each file on the computer"). Cf. United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009) ("[I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders," though officers should "first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure."). A few cases have held, based on the particular facts involved, that it was unreasonable to believe that the objects of the search would be found in certain files on the computer. See, e.g., United States v. Kim, 677 F.Supp.2d 930 (S.D. Tex. 2009) (search of encrypted JPEG files with names suggestive of child pornography not authorized by warrant permitting a computer to be searched for evidence of computer intrusion; in light of various facts, not reasonable to believe that the encrypted files would contain evidence of computer intrusion; thus, child pornography that was actually found was not in plain view).

B. Plain view

Given that computer search warrants typically allow officers to search every file on a computer, officers often encounter evidence of crimes other than those based on which the warrant was issued. For purposes of the following discussion, assume that the warrant was issued based on probable cause that the defendant committed financial crimes, and in the course of searching for evidence of those crimes, the officer found child pornography on the computer.

Several issues arise from this fact pattern. First, does the plain view doctrine apply to the image or images of child pornography initially encountered by the officer? Second, must the officer obtain a second warrant to continue searching the computer for additional evidence of child pornography? Or, because the original warrant likely permits a search of every file on the computer, may the officer simply continue rummaging?

These issues have divided the courts. Some courts have held that the plain view doctrine applies to the initial images, and that the officer may continue searching the computer under the original warrant, even if the officer subjectively hopes to find additional child pornography. These courts reason that the original warrant authorized the officer to inspect every file on the computer, and that the officer's motives

in continuing to search are irrelevant under settled Fourth Amendment case law. See generally, e.g., Brendlin v. California, 551 U.S. 249 (2007) ("[W]e have repeatedly rejected attempts to introduce this kind of subjectivity [looking at officers' motives] into Fourth Amendment analysis."). Cases in this group include United States v. Williams, 592 F.3d 511 (4th Cir. 2010) (defendant sent anonymous emails to a church expressing a sexual interest in some boys who attended school at the church; police obtained search warrant for "computer systems and digital storage media" indicative of computer harassment or communicating threats; during search, police found child pornography; child pornography was an "instrumentality" of the computer harassment charge and so was properly seized under the warrant; alternatively, because a computer search requires "at least a cursory review of each file on the computer," the child pornography was in plain view; the court applies the plain view doctrine as traditionally understood, notwithstanding the large amount of data that may be stored on a computer), and United States v. Mann, 592 F.3d 779 (7th Cir. 2010) (officer obtained search warrant to search the defendant's computer for evidence of voyeurism; he properly searched the image files on the computer systematically, even though he thereby uncovered child pornography; however, court found it "troubling" that he did not stop and seek a second warrant for child pornography).

Other courts have held that the plain view doctrine applies to the initial images, but that if the officer wishes to continue looking for child pornography, a second warrant is required. The leading case in this category is United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (officer obtained search warrant for "evidence pertaining to the sale and distribution of controlled substances"; officer opened .jpg file with sexually suggestive name, apparently because the file could contain a photograph related to drug activity; it contained child pornography; officer continued viewing other .jpg files with sexually suggestive names, finding more child pornography; although the first image was in plain view, by "the officer's own admission . . . each time he opened a subsequent [image] file, he expected to find child pornography and not material related to drugs," so the plain view doctrine did not apply).

Finally, some courts have indicated that the plain view doctrine should be limited, or perhaps even eliminated, in the context of computer searches, suggesting that even the initial images may not be admissible. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc) (noting that "over-seizing is an inherent part of the electronic search process" and suggesting that magistrate judges issuing search warrants should take steps to limit the government's access to data for which it has no probable cause, such as requiring an on-site assessment of the feasibility of seizing only responsive data; requiring data segregation to be done by someone other than the case agent; and perhaps limiting the government's plain view rights; Judge Kozinski's concurrence provides more detailed suggestions); In re United States's Application For A Search Warrant To Seize and Search Electronic Devices From Edward Cunnius, __ F.Supp.2d __, 2011 WL 991405 (W.D. Wash. Feb. 11, 2011) ("Because the government, in this application, refuses to conduct its search of the digital devices utilizing a filter team and foreswearing reliance on the plain view doctrine, the Court denies the application as seeking an overbroad or general warrant in violation of the Fourth Amendment").

VII. Special Cases

A. Searching computers that may contain privileged material

Special care must be taken when searching computers that may contain privileged material, such as a computer at an attorney's office or in a medical practice. One solution is to seize the computers, then have a special master, not employed by the police or the prosecutor's office, do the search. See, e.g., United States v. Hunter, 13 F.Supp.2d 574 (D. Vt. 1998) (suggesting this procedure, though approving as a less-satisfactory alternative having the search done by officers not involved in the investigation at issue). Alternatively, a procedure may be established by which claims of privilege are resolved among the defense, a "taint team" working for the prosecution, and the court. See, e.g., United States v. Triumph Capital, 211 F.R.D. 31 (D. Conn. 2000).

B. Issues regarding multiple residents or multiple users

Sometimes the police will seek authorization to search a shared computer, or all computers in a shared residence. Such requests raise questions. For example, if two users share a computer, and the police have probable cause to believe that one of them has committed a crime of which evidence can be found on the computer, may the police search the entire computer? Even if the users have separate password-protected accounts? And, if several residents of an apartment establish a computer network, does probable cause to search one resident's computer entail probable cause to search the other computers? Few cases bear on these questions. Cf. United States v. Greathouse, 297 F. Supp. 2d 1264 (D. Or. 2003) (police obtained a warrant to search the computers at a specific residence for child pornography; upon entering, they determined that several people lived at the residence, including the defendant, who had his own bedroom with a "Do Not Enter" sign on the door; the court held that the defendant's bedroom was essentially a separate residence, for which a separate warrant was required).

VIII. Returns and Inventories

Under G.S. 15A-257, an officer who executes a search warrant must return the warrant to the clerk without unnecessary delay. The return is indicated on the warrant itself. See AOC-CR-119. The officer must also provide the clerk with "a written inventory of the items seized," G.S. 15A-257, and a list of the items seized must also be provided to the person from whom they were taken, G.S. 15A-254. Form AOC-CR-206 may be used for creating an inventory.

With computer searches, a timing issue frequently arises. Suppose that a warrant authorizes officers to search a defendant's home and computer for evidence of a crime, and further allows the officers to conduct the computer search off-site. The search of the home and the seizure of the computer will likely take place shortly after the issuance of the warrant, but the search of the computer may not take place until later. Should the warrant be returned after the search of the home, or should it wait until the search of the computer is complete? And should the inventory list the computer itself, or the files and data within the computer?

No North Carolina cases answer these questions. The prevailing practice appears to be to return the warrant after the initial search, even if the computer has not yet been subjected to an off-site

examination. One justification for this practice is that it provides evidence of compliance with the requirement that a warrant be executed within 48 hours of issuance. G.S. 15A-247.[6] An inventory is normally provided at the same time, simply listing the computer as an item seized, and making no reference to specific data or files within the computer. This is probably sufficient, notwithstanding the fact that, as noted in Section V.C, above, the items to be seized under most computer search warrants are files and data rather than hardware. See Com. v. Kaupp, 899 N.E.2d 809 (Mass. 2009) (sufficient to return warrant shortly after initial search and prior to forensic examination "listing the devices" seized); United States v. Hernandez, 183 F.Supp.2d 468 (D. Puerto Rico 2002) ("[B]ecause off-site computer searches are reasonable, it may be necessary . . . for the return of the warrant to be filed with the court before such off-site searching can be completed."). An extremely cautious officer might file a supplemental inventory listing the data or files seized after the off-site search of the computer. In any event, however, imperfect compliance with the return and inventory requirements is unlikely to require the suppression of evidence. Cf. State v. Fruitt, 35 N.C. App. 177 (1978) (failure to leave a receipt with the person from whom property was seized violated statutory law but did not require suppression); Wayne R. LaFave, Search and Seizure § 4.12 (4th ed. 2004) (noting that most courts have declined to suppress evidence based on noncompliance with inventory or return requirements).

[6] The fact that the execution of the warrant is not complete within 48 hours, because the computer has not been examined, is probably immaterial. See, e.g., United States v. Cameron, 652 F.Supp.2d 74 (D. Me. 2009) ("[T]he Court concludes that so long as the search warrant was timely executed and the computer and the discs were seized within the period the warrant stipulated, the continued forensic inspection of the computer and the discs did not violate the Fourth Amendment, [the criminal procedure rules], or the conditions of the search warrant itself.").