Search Warrants for Digital Devices

Jeff Welty
UNC School of Government
August 2014

The United States Supreme Court recently observed that digital devices "have become important tools [for] . . . criminal enterprises, and can provide valuable incriminating information about dangerous criminals."[1] Law enforcement officers and prosecutors need to know how to obtain that information lawfully, so that it may be used in court. But the rules for digital searches sometimes differ from those for physical searches, and the law regarding digital searches is evolving rapidly. This document is a practical guide to obtaining and executing a valid search warrant for a digital device.[2]

A warrant is normally required to search a digital device. Under most circumstances, individuals have a reasonable expectation of privacy in the contents of their digital devices, such as cell phones, tablets, and computers. Therefore, the Fourth Amendment requires a law enforcement officer to obtain a search warrant to search such a device, unless an exception to the warrant requirement applies. The Supreme Court recently eliminated one important exception when it held that a digital device may not be searched incident to a suspect's arrest.[3] Thus, a search warrant will often be necessary to search a suspect's digital devices.

Establishing probable cause. A warrant, of course, requires probable cause. In general, probable cause to search a digital device is no different from probable cause to search a physical object or location. But there are a few probable cause issues that are unique to digital searches.

Probable cause may be based on an IP address. Investigators sometimes determine that criminal activity has been conducted through a particular Internet Protocol address, or IP address, and are able to trace the IP address to a residence, only to learn that the residence has an unsecured wireless network. In such a case, investigators may be unable to rule out the possibility that a neighbor or a passer-by, rather than a resident, used the network for criminal purposes. Nonetheless, courts have generally ruled that there is probable cause to search the digital devices at the residence, as residents are the most likely users of the network.[4]

---

[1] *Riley v. California*, __ U.S. __, 134 S.Ct. 2473, 2493 (2014).
[2] For more detail, see Jeffrey B. Welty, *Digital Search and Seizure* (UNC School of Government forthcoming 2015).
[3] *Riley*, *supra.* By its terms, *Riley* applies only to cellular phones, but its reasoning plainly applies to digital devices more broadly.
[4] *See*, *e.g.*, *United States v. Vosburgh*, 602 F.3d 512, 526 (3d Cir. 2010) ("[E]vidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address."); *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (though use of an unsecured wireless connection would make it possible that a transmission of child pornography could have originated from outside of defendant's residence, the court rejected defendant's argument that "the association of an IP address with a physical address does not give rise to probable cause to search that [physical] address"). *See also United States v. Thomas*, 2012 WL 4892850, *4 (D. Vt. Oct. 15, 2012) (unpublished) ("[C]ourts have generally

Probable cause in child pornography cases. Courts have addressed a number of recurrent issues that arise in child pornography investigations. In general:

- When probable cause is based on a witness having seen child pornography on a suspect's digital device, the officer who applies for the search warrant should provide an explicit and detailed description of the images or videos seen by the witness.[5] If the officer simply describes the material as "child pornography," a judicial official may be unable to make an independent determination about the nature of the material and the existence of probable cause.
- When probable cause is based on information that a suspect had child pornography on his digital devices weeks or months in the past, an officer with experience in child pornography investigations should explain in the search warrant application that individuals who view child pornography tend to retain it. When presented with such information, courts often recognize that information that a suspect has child pornography on his or her digital devices does not easily become too outdated, or "stale," to support a search warrant.
- Where there is evidence that a suspect has had sexual contact with children or has visited non-pornographic web sites oriented towards pedophiles, these facts may help to support a finding of probable cause to believe that child pornography will be present on the suspect's digital devices. However, these facts alone may not be sufficient to provide probable cause.[6]

Drafting warrant applications and proposed warrants. Several practices should be followed when drafting search warrant applications and proposed search warrants for digital devices.

Include digital-specific language. The Fourth Amendment requires that a warrant describe the place to be searched with particularity. If a warrant identifies a physical location, such as a suspect's home or office, without specifically mentioning digital devices that may be present, there may be some doubt about the sufficiency of the warrant to authorize the search of the devices. Several courts have ruled that such a warrant is adequate, because a warrant authorizing the search of a particular location for a particular item generally authorizes the search of any container at the location that might reasonably contain the evidence sought, and digital devices are containers for information.[7] So, for example, a warrant authorizing the search of a home for records of drug sales, lists of drug customers, and the like would allow the search of any drawer or box within the home in which the records could reasonably be found, *and* the search of any computer or cell phone that could contain such records.[8] However, a few

---

concluded that the mere possibility that an IP address may be associated with an unsecure wireless network does not affect the probable cause determination.").

[5] In the alternative, the officer might attach the material under seal, if the officer has access to the material.

[6] For case citations on these issues, see Jeffrey B. Welty, *Digital Search and Seizure* (UNC School of Government forthcoming 2015).

[7] 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).

[8] *See*, *e.g.*, *State v. Gurule*, 303 P.3d 838 (N.M. 2013) (because a digital camera was a potential "container" for child pornography images, a search warrant authorizing the search of a suspect's home for such images supported the seizure and search of the camera; there was no need for an officer to seek a second search warrant); *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008) (holding that a search warrant authorizing a search for "documents,"

courts have suggested that digital devices are different and normally may be searched only if specifically permitted by the warrant.[9] Therefore, a cautious officer who anticipates needing to examine digital devices should note that fact in the application and provide for it in the proposed warrant. Officers should also seek authorization to seize manuals, power cables, and passwords associated with digital devices, as not having these items may make a forensic search difficult or even impossible.

Describe the items to be seized in as much detail as reasonably possible. The Fourth Amendment requires that a warrant describe the items to be seized with particularity. In most cases involving digital devices, the devices themselves are incidental to the true object of the search, which is the information contained on the devices. Thus, a warrant application should describe the files or information sought, not merely the devices, and should do so as specifically as reasonably possible. At a minimum, it should link the material sought to a specific offense. A court may view as overbroad a warrant that authorizes the seizure of all digital devices that belong to a suspect, but is likely to approve of a warrant that authorizes the seizure of all digital devices that belong to the suspect *and that could contain evidence of the specific crime under investigation*.[10] In an appropriate case, the description of the items to be seized could be further tailored by limiting the files to be examined to files created or accessed by a specific user, or to files created or accessed on or after a specific date.

Include authorization for off-site forensic analysis. In theory, a suspect's digital devices could be searched at the location where they are seized. In practice, the massive storage capacity of modern digital devices and the need to use specialized forensic tools to examine them makes it more practical to search such devices in a laboratory setting. Therefore, the application should explain that officers plan to seize the suspect's digital devices and take them off-site for copying and forensic analysis, and the warrant should authorize this procedure.[11] It is a good idea to make clear that this process will be time-

---

without mentioning computers or electronic storage, allowed police to search computers, as documents may be found in computers).

[9] *United States v. Payton*, 573 F.3d 859 (9th Cir. 2009) (suggesting that computer-specific language normally is required before digital devices may be searched pursuant to a warrant)

[10] *Compare United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013) (officers suspected a registered sex offender of failing to disclose his online identifiers as required by law and of luring young boys to his home; they obtained a search warrant that authorized the seizure and search of the offender's computers and other digital devices for evidence of violations of "NYS Penal Law and or Federal Statutes"; this was insufficiently particular as it did not limit the items to be seized to those connected to any specific crime; the court stated that the "particularity requirement assumes even greater importance" with digital searches as "advances in technology . . . have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain"), *and 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 house, without any mention of any particular crime to which they might be related" lacked particularity), *with United States v. Christie*, 717 F.3d 1156 (10th Cir. 2013) (noting that application of the "Fourth Amendment's particularity requirement to computer searches [was] still relatively new" but identifying as a "recognizable line" the notion that warrants lacking a "limiting principle" tend to be invalid, while warrants which are limited in their scope to either evidence of a specific crime or evidence of a particular type of material tend to be valid).

[11] *See United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad."); *United States v. Mutschelknaus*, 592 F.3d 826 (8th Cir. 2010)

consuming and will not be completed within 48 hours of the issuance of the warrant. That will help to alleviate any concerns about the requirement that a search warrant be executed within 48 hours of issuance, an issue discussed further below.

Do not include a search protocol. Because digital files can be camouflaged or disguised through misleading file names or extensions, it may be necessary to examine every file on a digital device when searching for incriminating material. Officers often use keyword searches, hash value searches, and other automated searching techniques to facilitate this process. An influential Ninth Circuit opinion has suggested that the search protocol that officers plan to use should be described in the warrant application, so that a judicial official may assess whether the search protocol is likely to retrieve only relevant material.[12] However, most courts have held that a search protocol need not be included.[13] As one court stated, "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic."[14] The United States Department of Justice advises federal officials not to include any "[l]imitations on search methodologies" in the warrant or application.[15] In light of this recommendation and the weight of authority, officers should not include a specific search protocol in a warrant application.

Present the application to an appropriate judicial official. Any judicial official empowered to issue search warrants may issue search warrants for digital devices. However, there are circumstances under which a cautious officer handling a serious case may prefer to submit a search warrant application concerning a digital device to a superior court judge. First, a warrant from a superior court judge is valid throughout the state.[16] Where the officer plans to submit the device to a laboratory in another part of the state, such as the state crime laboratory, obtaining a warrant that is valid statewide may avoid any question about whether the warrant properly authorizes the laboratory search. Second, if the officer is seeking a warrant for a new type of device or a new type of digitally-stored information, a judge may be better

---

(warrant allowing officers 60 days to conduct off-site examination of seized computer was reasonable given the complexity of computer searches); *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).

[12] *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring).

[13] *United States v. Evers*, 669 F.3d 645, 653-54 (6th Cir. 2012) (a warrant was not unconstitutional due to its "failure to describe with particularity the computer files to be searched or to require the use of a search protocol" because the warrant "confined the search to evidence of child pornography on the computer, camera, and media described by the victim"); *United States v. Cartier*, 543 F.3d 442, 447 (8th Cir. 2008) (a search warrant was not invalid per se due to its lack of search protocol); *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.").

[14] *United States v. Burgess*, 576 F.3d 1078, 1093 (10th Cir. 2009).

[15] United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching Computers and Obtaining Electronic Evidence in Criminal Investigations* 79 (2009).

[16] G.S. 15A-243. Search warrants issued by district court judges are valid throughout the district, and search warrants issued by magistrates are valid throughout the county. *Id.*

suited than a magistrate to identify possible legal problems with the warrant. Finally, some federal prosecutors reportedly have expressed a preference for warrants to be signed by superior court, so if the case may be referred for federal prosecution, the officer may prefer to present the warrant to a judge.

Executing the warrant.

Handle digital devices properly. The North Carolina State Crime Laboratory Evidence Guide provides guidelines on handling digital devices properly during a search. It addresses issues such as whether to leave devices on or turn them off, and whether to shut devices down normally or simply unplug them. Officers who are unfamiliar with searching digital devices should review the guide. They may also contact the local SBI district office and ask to speak to a member of the computer crimes unit for advice.

Comply with timing requirements. Under G.S. 15A-248, "[a] search warrant must be executed within 48 hours from the time of issuance." It likely is sufficient if the initial seizure of the digital devices is completed within this time period, even if the subsequent off-site forensic analysis takes longer. Concerns about the 48-hour rule may be reduced by obtaining explicit authorization in the warrant for a laboratory forensic analysis, as discussed above. Still, some courts have criticized extremely long delays in examining digital evidence, so any forensic analysis should be completed promptly.[17]

Obtain a second warrant when evidence of another crime is found. When an officer obtains a warrant to search a digital device for evidence of one crime, but stumbles on evidence of another, the officer should obtain a second warrant authorizing a search of the device for the second crime. Arguably, this is unnecessary: because it is impossible to know what a given file contains without examining it, most courts would allow the officer to search every file on the device for evidence of the first crime, rendering all the evidence of the second crime in plain view. However, one federal court of appeals has ruled that a warrant is necessary when an officer changes the focus of his or her search of a digital device,[18] and

[17] *See*, *e.g.*, *United States v. Ganias*, __ F.3d __, 2014 WL 2722618 (2d Cir. 2014) (finding a Fourth Amendment violation and reversing the defendant's conviction where the Government did not examine the defendant's computers until eight months after seizing them, and ultimately retained them for over two years; "[t]he Government's retention of copies of [the defendant's] personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time"); *United States v. Cote*, 72 M.J. 41 (U.S. Ct. App. Armed Forces 2013) (computer search warrant provided that the initial search was to be executed within 10 days and that any forensic analysis of a seized device was to be completed within 90 days, but officers conducted a forensic examination of a seized hard drive more than a year after the warrant issued; "the Government's violation of the warrant's time limits for conducting an off-site search of the seized electronic device constituted more than a 'de minimis' violation of the warrant and resulted in an unreasonable search"; court suggests in a footnote that even absent the explicit time limit in the warrant, the Fourth Amendment's reasonableness requirement may be implicated by such a long delay). The Federal Rules of Criminal Procedure recognize that "[a] warrant [that] authorize[s] the seizure of electronic storage media or the seizure or copying of electronically stored information . . . . authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B).

[18] *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;

another has called into question the use of the plain view doctrine in searches of digital devices.[19] Because the law in this area is unsettled, obtaining a second warrant is prudent.

Dealing with password protected devices. Digital devices, especially cellular phones, may be password protected. In some cases, officers with training in digital forensics may be able to bypass the password. In other cases, the manufacturer of the operating system may be able to extract some information from the device despite the password. This may require obtaining an additional search warrant to be served on the manufacturer. For example, Apple can extract "SMS, photos, videos, contacts, audio recording, and call history" from locked iPhones, but will do so only pursuant to a search warrant containing the specific language contained in Apple's law enforcement guidelines.[20] However, because password protection may make it more difficult, or even impossible, to access the information on a digital device, officers should (1) seize any papers near the devices that may contain passwords, and (2) attempt to prevent active devices from shutting down or "sleeping" such that entry of a password is required to activate the devices.

Expect technical limitations. Enormous amounts of information may be extracted from digital devices. For example, cell phones may contain GPS location information, and computers may contain recoverable deleted files. But devices vary, and digital evidence technicians warn that some will bear more fruit than others, depending on storage capacity, operating system, security features, and other factors.

Preparing the return and inventory. Under G.S. 15A-257, an officer who executes a search warrant must return the warrant to the clerk without unnecessary delay. The return normally is indicated on the warrant itself.[21] The officer must also provide the clerk with "a written inventory of the items seized,"[22] and a list of the items seized must also be provided to the person from whom they were taken.[23] Form AOC-CR-206 may be used for creating an inventory. Searches of digital devices present several issues regarding returns and inventories.

Make the return after the initial seizure. Should the warrant be returned after the initial seizure of a suspect's digital devices, or should it wait until the subsequent forensic analysis is complete? There is no North Carolina case on point, but the prevailing practice is to return the warrant after the initial seizure of the suspect's devices, even if the devices have not yet been subjected to an off-site examination. One

---

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). *But see United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) (noting that "we have not required a specific prior authorization along the lines suggested in *Carey* in every computer search").

[19] *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring) ("When the government wishes to obtain a warrant to examine . . . [an] electronic storage medium . . . magistrate judges should insist that the government forswear reliance on the plain view doctrine.").

[20] Apple, Inc., *Legal Process Guidelines: U.S. Law Enforcement*, https://www.apple.com/legal/more-resources/law-enforcement/.

[21] See AOC-CR-119.

[22] G.S. 15A-257.

[23] G.S. 15A-254.

justification for this practice is that it provides evidence of compliance with the requirement that a warrant be executed within 48 hours of issuance.[24]

List the devices themselves on the inventory, at least initially. Another question is whether the inventory should list the devices themselves, or the files and data within the devices. Because officers generally complete an inventory at the same time as documenting the return of the warrant, the prevailing practice is to list the digital devices as items seized, making no reference to specific data or files, which often have not been extracted at this juncture. This is probably sufficient, though a cautious officer might file a supplemental inventory listing the data or files seized after the off-site search of the devices. In any event, imperfect compliance with the return and inventory requirements is unlikely to require the suppression of evidence.[25]

Special cases. Special problems arise when searching digital devices that belong to third parties not suspected of any crime; when searching digital devices that contain privileged material, such as devices that belong to attorneys or physicians; and when searching digital devices that belong to the news media, broadly defined. A full discussion of these situations is beyond the scope of this paper, but the references cited in the footnotes may be helpful.[26]

Getting help. Officers and prosecutors who need assistance with search warrants for digital devices have several options:

- Jeff Welty, UNC School of Government, (919) 843-8474, welty@sog.unc.edu (help with legal issues)
- State Bureau of Investigation, Computer Crimes Unit (available by calling local district office) (help with legal and technical issues)
- State Crime Lab, Digital Evidence Section, (919) 662-4500 (help with technical issues)

Sample search warrants for computers and electronic devices are available in several locations, including:

[24] G.S. 15A-247. 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.").

[25] State v. Nadeau, 1 A.3d 445 (Me. 2010) (computer search warrant provided that the search was to be conducted, and an inventory returned, within 10 days; no inventory was ever prepared, but this was a "ministerial" failure that did not warrant suppression of evidence); State v. Fruitt, 35 N.C. App. 177 (1978) (officer's failure to comply strictly with inventory requirement did not require suppression of evidence).

[26] United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009). *See also* Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 Yale J. L. & Tech. 311 (2009-10).

- United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) (appendices contain sample warrants)
- Heart of America Regional Computer Forensics Laboratory, http://www.harcfl.org/DSP_L_warrants.cfm