The Legal Aspects in Obtaining Digital Evidence: Revisiting Principles of the Fourth Amendment in the Digital Era

Tri Dai Ho

School of Cyber Education, UMGC-Global

CCJS 321-7382: Digital Forensics in the Criminal Justice System

Professor Maurice Hicks

4th March 2023

1. Describe search warrants and how they can be used to obtain digital evidence by specifically answering each of the following questions:

a. List each of the requirements of a search warrant articulated in the United States Constitution's bill of rights and how in practice, the police investigator can/does comply with those requirements to obtain a search warrant.

The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

According to Wex Definition Team (2022) from Legal Information Institute (LII), a search warrant is a warrant that authorizes law enforcement officers to search for a specific person, a specified place, or an automobile for evidence of a violation. Specific requirements must be met for a search warrant to be legally issued and carry legal weight. The search warrant seeker must testify that the warrant is based on probable cause, with specific particularity, and signed by a magistrate or judge. LLI provides a more detailed view of each of these requirements.

Probable cause: The officer needs to justify a reasonable belief that evidence of illegal activities can be found based on supported information from personal observation or an informant.

Particularity: The warrant should describe the place to be searched and the things to be seized with particularity.

Signed by a "neutral and detached" magistrate or judge (Wex Definitions Team, 2022).

In practice, the law officer is still required to execute the search in a manner that abides with the principle of the Fourth Amendment. They are:

Object: The warrant should be executed by government officers. Private citizens cannot execute it (Wex Definitions Team, 2022).

Timing: If an unreasonable delay occurs, causing the warrant not timely executed, the grounds that probable cause may disappear. The warrant usually does not execute at night and should occur between 6:00 a.m. and 10:00 p.m., except in some exceptional circumstances (Wex Definitions Team, 2022).

Manner: Knock-and-announce rule: When searching a certain place, an officer must knock and announce authority and purpose before entering, and should wait for a reasonable time or be refused admittance before using force to enter. Waiting time could be several seconds or not required, if the officer has reasonable fear or suspicion that evidence will be destroyed, or the investigation will get inhibited. Failure to knock and announce will not cause the suppression of evidence (Wex Definitions Team, 2022).

Extent: During the conduction of a search, the officer cannot search the places and individuals not listed on the warrant. However, the officer may detain or arrest anyone present during the search if they find sufficient evidence (Wex Definitions Team, 2022).

b. Discuss how a search warrant can be used to obtain digital evidence.

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review (Rule 41. Search and Seizure, n.d.-b).

Rule 41(e)(2)(A) dictates that a search warrant must include a time cap to which the computer and electronic storage media were seized within the ten (10) day time limit following the issuant of a search warrant. Digital Search Warrants - Law Enforcement Cyber Center (2018) further elaborated that forensic analysis must be performed within the sixty (60) days granted by the magistrate judge… [T] the Federal Rules of Criminal Procedure do not require the forensic analysis of

computers and other electronic equipment to occur within a specific time limit but only in a reasonable time.

For tracking the device, the warrant must include the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable time for the device. The time must be 45 days from when the warrant was issued. For a good cause, the court may grant one or more extensions for a reasonable period not exceeding 45 days each (Rule 41. Search and Seizure, n.d.-b).

2. Explain the steps from obtaining the search warrant in which digital evidence is sought to having the digital evidence in a format presentable in court.

The steps that require law enforcement to obtain a search warrant for digital evidence are the following:

1. Establishing a probable cause sets the reason for a search. A probable cause is made up of supported information either by investigation means, tips from informants, or previously collected evidence leading the officer to believe in the evidence that can be obtained from digital data, or physical hardware that contain such data.
2. Presenting the case to the court: The officer can justify this probable cause with the judge or through a reliable media channel. Either way, they still need to fill out an application to obtain a search warrant. In this application, the officer must present all known factors thus far that provide them with a reasonable belief that a search for or seizure is necessary. The officer also needs to provide the specific type of data or device that will be inspected or seized from whom or where in reasonable detail.
3. The officer must specify the period needed to properly analyze the data, provide any potential setback, or variation of said period and provide a possible reason why this may occur.

3. **Explain how the Plain View Doctrine and Exigent Circumstances may apply to digital evidence. Be sure to address the Plain View Doctrine and the three requirements an officer must fulfill to claim they successfully operate under it.**

Plain view doctrine is one of the few exceptions where a search warrant is exempt from seizing the evidence. According to Richert (n.d), the plan view doctrine exists out of the officer's convenience to obtain exposed evidence in plain view. For the office to obtain evidence under this doctrine legally, three requirements must be met:

- **Presence of probable cause,** like in a regular search with a warrant.
- **Prior valid entry** means that the officer must be legally present in the area before the seizure.
- **Inadvertence** This means that the evidence obtained under plain view doctrine must be of "element of surprise" or not intentionally sought by the officer (Richert, n.d).

Let us consider two examples to illustrate the idea behind the plain view doctrine. It is illegal in most states to have a firearm locked and loaded and lay openly within the arm's reach of the driver. If the police stop a car for a traffic violation, and upon approaching the vehicle, the officer sees the weapons with a magazine, not in any form of a case. Even though the officer was initially there for a traffic violation, the officer has the legal grounds to seize the weapon and detain the driver. Now let us consider another case that does not align with the plain view doctrine. In the same situation, if said firearms still lock and loaded with magazines, but in a close case. The officer may have a reason to suspect the weapon may be loaded, but since it is not visible from eyes sight, the officer cannot seize the weapon under plain view doctrine.

a. **Describe a scenario in which an officer may claim the plain view applies to digital evidence—what might be an applicable counterargument in court?**

   The unique property of digital data, especially when serving as evidence, is that it typically binds or links to an event that takes place in the physical world, but it (the digital data) only

exists in the virtual world. As indicated by Ward (2011), our current legal system often switches back and forth between two concepts:

1. Treat digital data as physical evidence since a storage device must be used.
2. Treat digital data as its entities where each data type is an independent unit.

In *United States v. Williams* (2010), the Fourth Circuit applied the plain view doctrine, allowing child pornography obtained during the execution of a warrant for a separate crime to be used against the defendant. In this case, the police already possess a legal warrant to search the content of the computer system, digital storage media, and other instruments used by the defendant (*United States v. Williams*, 2010). The Fourth Circuit decided that the child pornography material fit the three requirements of the plain view doctrine.

- Probable cause: Threat emails were sent by a computer, leading the police to believe a search of the defendant's device will either prove or deny the suspect's connection to the crime.
- Valid prior entry: The police were present with a warrant allowing for the search and seizure of electronic instruments and media storage that can be used to commit the crime.
- Inadvertence: The police did not intend to seize child pornography material but came upon the material while executing the warrant.

While treating data according to the limitation of its physical carrier upholds the concept of the plain view doctrine, this interpretation can be effectively challenged using the second concept, where data need to be treated as entities.

1. A machine or device is used to read the data, which can be seen as the officer making a deliberate effort to view the object but not stumble upon it. This invalidates the inadvertence requirement (Ward, 2011).

2. Since the officer cannot view the content without opening them, this invalidates the concept that they are in plain view (Ward, 2011).
3. None of the folder or files name bear any term or meaning that lets the officer reasonably believe that it may contain the evidence. This may add to the inadvertence but detracts from the probable cause requirement (Ward, 2011).

4. Explain the exigent circumstances doctrine and the category of circumstances that qualify as exigent circumstances under the doctrine.

The essence of the exigent circumstances doctrine very much aligns with the old saying, "Desperate time calls for desperate measure." This doctrine is designed to assist and provide the legal ground with limited freedom for the officer to act in the heat of the moment. The exigent circumstances doctrine allows an immediate search and seizure without a warrant if the officer can justify the necessity of the seizure, the urgency nature of the situation, or the strenuous circumstances to which it is illogical to return with a search warrant. As defined in *United States v. McConney* (1984) by Wex Definition Team (2022), exigent circumstances are situations that require a rapid action to

1. Prevent physical harm to the officer or person.
2. Destruction of relevant evidence
3. Escape of the suspect
4. Other instances inhibit legitimate law enforcement efforts.

In *United States v. Vaatausili Mark Alaimalo (2002),* as cited in Champlin et al. (2015), the officer was aware of a common practice where illegal drug dealers immediately divide up the drug upon receiving one. In conjunction with all other prior evidence, this led the officer to legitimate concerns about the destruction of evidence, the safety of others, and the potential runaway suspect. The officer made a warrantless entry and seized the drug in plain view. This is a prime

example of exigent circumstances. In another example, Web Definition Team (2022) states that the officer can detain the suspect before obtaining the warrant in hot pursuit.

a. Describe a scenario in which an officer may claim that the exigent circumstances doctrine applies to digital evidence—what might be an applicable counterargument in court?

In *United States v. Meyer* (2021), as cited in Daigle (2023), the government agents obtained the computers and cell phones that Meyer used to contact and transfer money to a child pornography distributor in the Philippines. Also, in this case, the agent knew that Meyer (1) had ties to the individuals who were live-streaming sexual abuse of children; (2) had stayed with these individuals when he visited the Philippines; (3) had paid thousands to them and one of the minor victims; and (4) did not tell his wife about some of the money he sent, despite claiming that the payments were tied to his humanitarian work. This known evidence is probable cause for the agent to believe the existence of the material (Daigle, 2023). Furthermore, Daigle (2023) pointed out that the agent reasonably suspects that if they were to wait for the search warrant, Meyer could clear up his hard drive or destroy the device since the defendant made the repetitive notion of "having to do some clear up first."

Some applicable counterarguments for this case can be:

1. Even with exigent circumstances established, the hardware device that stored the material is presumably located in a home office or bedroom. The expectation of privacy in these areas are higher and does not consider plain view since the officer would need to open more than one door to search or seize. If the material was not actively playing on the computer, there is no probable cause to seize them. Exigent circumstances limit the officer to a quick scan without a warrant and not a thorough search. The act of opening more than one set of doors and entering a more private area can be considered a thorough search.

2. There is a clear possibility that Meyer could have deleted the evidence while waiting for the warrant. However, the digital forensic team has the tool to recover deleted files, and bank transactions could be obtained from the banks with a warrant. The illegal content was live streaming to the defendant, meaning even if Meyers were to destroy the hardware to the point of unrecoverable, IP tracking with data server logs could still review the connection between the child pornography distributor. The officer could have waited for the warrant approval instead of entering. In this manner, the agent's entry was uncalled for since the legal alternative was present that could secure the same evidence.
3. There was no immediate threat, and Meyers complied with most of the officer's requests on the scene. When Meyer gave verbal consent to turn in his phone examination, there was no need to seize the device. As mentioned above, files are considered truly deleted only when other content is already written on the same slot in the drive cluster.

References

Champlin, K., Oldham, C., & Salvatoriello, P. (2015, December 14). Exigent circumstances - definition, examples, cases, processes. In *Legal Dictionary*. Retrieved April 3, 2023, from https://legaldictionary.net/exigent-circumstances/

Daigle, E. (2023, March 14). *Exigent circumstances when handling electronics*. DLG Learning Center. Retrieved April 4, 2023, from https://dlglearningcenter.com/exigent-circumstances-when-handling-electronics/#:~:text=Exigent%20circumstances%20can%20arise%20even%20more%20in%20computer,can%20be%20triggered%20with%20just%20a%20few%20keystrokesWex Definitions Team. (2022, May). Search warrant. In *LII / Legal Information Institute*. Retrieved April 1, 2023, from https://www.law.cornell.edu/wex/search_warrant

Digital Search Warrants - Law Enforcement Cyber Center. (2018, September 13). Law Enforcement Cyber Center. https://www.iacpcybercenter.org/prosecutors/digital-search-warrants/

Richert, D. (n.d.). *Plain view doctrine | Office of justice programs*. ojp.gov. Retrieved April 3, 2023, from https://www.ojp.gov/ncjrs/virtual-library/abstracts/plain-view-doctrine

Rule 41. Search and Seizure. (n.d.-b). In *LII / Legal Information Institute*. Retrieved April 1, 2023, from https://www.law.cornell.edu/rules/frcrmp/rule_41#rule_41_e_2_A

Ward, K. (2011).The plain (or not so plain) view doctrine: applying the plain view doctrine to digital seizures. *University of Cincinnati Law Review*, *79*(3), 6. https://scholarship.law.uc.edu/uclr/vol79/iss3/6/

Wex Definitions Team. (2022, December). Exigent circumstances. In *LII / Legal Information Institute*. Retrieved April 4, 2023, from https://www.law.cornell.edu/wex/exigent_circumstances

United States v. Williams, 592 F.3d 511 (4thCir. 2010), cert. denied, 131 S. Ct. 595 (2010).

.